20 PLANNING REPORT

TECHNOLOGIES IN THE SERVICE SECTOR

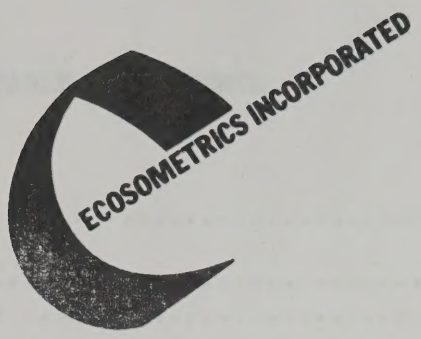
Volume III: A Case Study of Payment Technologies in Banking

Prepared by
Ecosometrics, Incorporated

October 1984

Program Office
National Bureau of Standards

NBS GCR 84-474-3



Research Report No. RR-174

TECHNOLOGIES IN THE SERVICE SECTOR: A CASE STUDY OF PAYMENT TECHNOLOGIES IN BANKING

VOLUME III

Final Report

Elliott E. Hamilton
Armando M. Lago

October 1, 1984

Prepared for:

Office of Planning
National Bureau of Standards
U.S. Department of Commerce
Gaithersburg, Maryland

Under Contract NB83SBCA2084

4715 CORDELL AVENUE • BETHESDA, MARYLAND 20814 301/652-2414

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	S-1
Study Objectives	S-1
Banking and Payment Systems	S-2
Check Processing	S-3
Wholesale Electronic Funds Transfer	S-8
Retail Electronic Funds Transfer	S-10
Encryption and Security Systems	S-16
Smart Cards	S-19
Home Banking	S-22
1 -- STUDY OBJECTIVES AND BACKGROUND	1
Study Objectives	1
Banking and Payment Systems	2
2 -- CHECK PROCESSING	5
Background	5
Productivity in Check Processing Operations	7
Barriers to Further Productivity Gains	13
3 -- WHOLESALE ELECTRONIC FUNDS TRANSFER	21
Background	21
4 -- RETAIL ELECTRONIC FUNDS TRANSFER	31
Background	31
Retail EFT Technology	36
Barriers to Adoption and Use of Technologies	47
5 -- ENCRYPTION AND SECURITY SYSTEMS	49
Background	49
Security System Components	52
Computer Vulnerability	55
Barriers to the Adoption and Use of Security Technologies	56
6 -- SMART CARDS	63
Background	63
Pilot Tests and Activities Worldwide	68
Barriers to Adoption and Use	71
Standards Activities and Technical Support Needs	73
Future Outlook	73
7 -- HOME BANKING	75
Background	75
Pilot Tests and Industry Participants	77
Market Projections	82
Barriers to Growth	84

EXECUTIVE SUMMARY

This case study of technologies related to payment systems in the banking industry is part of a larger study of technological trends in the service sector. Other portions of the study deal with general and technological trends in the service sector of the U.S. economy and with the emerging videotex/teletext industry.

STUDY OBJECTIVES

The objectives of this case study of payment systems in the banking industry are:

1. to develop data and information on the growth prospects of payment technology in the banking sector;

2. to assess barriers -- economic and technological -- to the adoption and use of these technologies; and

3. to identify to the extent possible the work on standards and technological support required in view of the expected growth.

The payment and electronic fund transfers technologies were identified as candidates for a case study in an analysis of technological trends in the U.S. service sector. The banking industry was identified as having one of the highest rates of growth among service sector industries. In addition, payment

system technologies were found to have important implications for the service sectors which interact directly with the consumer, such as retailing, among others.

BANKING AND PAYMENT SYSTEMS

The costs of administering and processing payments have been estimated as amounting to one percent of our Gross National Product,[1] with roughly two-thirds of this cost associated with using checks as a means of payment. A study conducted by Federal Reserve Bank of Atlanta[2] found that the growth in the number of checks written averaged between five and six percent annually from 1974 through 1979, and two percent per year from 1979 to 1983. This growth in the volume of checks to be processed is having a significant impact on the costs of doing business. The costs of processing checks by supermarkets amounts to close to 0.83 percent of sales, close to supermarkets' net margin rate of one percent.[3] Indeed the magnitude of the payments problem has attracted the interest and concern of the Federal Reserve Board and the banking industry to deal with this problem.

In 1980, the Depository Institutions Deregulation and Monetary Control Act phased out all the legally imposed interest rate ceilings paid on deposits and, in addition, enabled banks to unbundle the bank service charges for the processing of checks. With bank costs rising for check processing, banks are beginning to charge substantial fees for writing checks. Basic banking services for a household have increased from $90 in 1979 to over $180 a year in 1983, and now make up 24.8 percent of a bank's income as opposed to 19.2 percent in 1979.

The need to cope with the payments problem has made it necessary to create incentives for the adoption of technological changes that would enable handling of transactions in a more cost-effective manner. These payments-related technologies are discussed in this report; they include: check processing technology improvements, wholesale and retail electronic funds transfer (EFT) systems, security technology related to handling payments, Smart Cards and home banking.

---

[1]Arthur D. Little, Inc. The Consequences of Electronic Funds Transfer. Cambridge, Massachusetts. June 1975, p. 8.

[2]Quoted in "Displacing the Check". Federal Reserve Bank of Atlanta Economic Review. August 1983.

[3]"The Debit Card at The Crossroads". Federal Reserve Bank of Atlanta Economic Review. March 1983, p. 42.

Check processing involves a variety of operations such as encoding, reading/sorting, exception and return item processing, etc. The productivity of labor processing operations is presented in Table S-1, showing that the overall total productivity for check processing operations rose 5.1 percent in 1981 after remaining relatively stable during the previous two years. Productivity increases should continue as greater use is made of automated reject processing, bulk filing and check truncation, and as banking staff becomes more familiar with system operations. The productivity improvements noted, however, will only serve to maintain the status quo, as check volume is expected to grow until 1990.

As shown in Table S-1 the productivity of several operations has either not improved or actually deteriorated. These operations include: return item processing and reject processing, among others. Encoding is the most labor intensive function and the focus of productivity programs implementing incentive plans for inscriber operators.

Return item productivity decreased in the period 1978-1981, and was down to 48 items per man-hour in 1981. Productivity levels should improve as automated systems are introduced and the ANSI X9.3-1981 check endorsement specification standard is adopted by the major clearing banks. The standard calls for a uniform placement of endorsement on the back of checks and will eliminate the confusing overlap of multiple endorsement stamps.

The productivity level for reject processing reflects the fact that most banks still process rejects by manual methods. As automated reject processing is used more, productivity levels should increase.

Barriers To Further Productivity Gains

Literature reviews and limited contacts with banking equipment manufacturers and banking industry officials revealed some issues of concern that may bar the path to productivity gains in check processing operations. Because these issues concern measurements and tests, of interest to NBS, they are discussed next.

Table S-1

LABOR PRODUCTIVITY IN CHECK PROCESSING OPERATIONS OF COMMERCIAL BANKS
1978-1981

(Average Checks Per Man-Hour)

Check Processing Operations	1978	1979	1980	1981
Balancing and Correction	2,559	2,456	2,880	3,218
Encoding Operations	928	859	865	876
• single-pocket machine	845	881	864	920
• multipocket machine	657	628	686	767
Check Receiving	N.A.	N.A.	6,519	8,970
Reader/Sorter Operations	12,423	12,527	11,740	13,044
Cash Letter Make-Up and Microfilming	7,262	6,261	6,323	6,215
• cash letter make-up	5,626	5,557	5,768	5,484
• microfilming	11,130	12,609	7,933	8,970
On-us Paying, Filing and Return Item Processing	831	1,066	965	824
Exception and Return Item Processing	26	34	27	24
• exception item processing	3	3	3	3
• return item processing	N.A.	85	54	48
Bulk Filing	N.A.	N.A.	N.A.	4,423
Reject Processing	297	309	308	248
Overall Labor Productivity	523	530	525	552

N.A. represents lack of comparable data availability

Source: Bank Administration Institute. 1981 Survey of the Check Collection System. Rolling Meadows, Illinois, 1982, pp. 28-41.

Measurement of Embossment Levels of MICR Line

The basis for the automation of check handling is the Magnetic Ink Character Recognition (MICR) line standard (ANSI X3.3-1970, revised in 1976). MICR encoding began appearing in 1958 arising out of a study conducted by the American Bankers Association (ABA). MICR encoding on the face of a check contains standard routing information, the amount of the check, the account number, and in-house codes.

A current concern of the banking industry is the level of embossment of the MICR line, which is the primary cause of reader/sorter rejects. The MICR line problem can be caused by either the check printer who place part of the MICR information on a check, or by the bank's own MICR encoding, such as for the dollar amount. The current embossment depth standard is for a 1/1000 inch tolerance level. A too severe embossment will either lower the MICR signal level to an unreadable level or will cause a character to be read incorrectly.

There are no means today for printers or banks to measure their embossment level because there are no commercially available measurement devices to verify the 1/1000 inch tolerance level. In fact, the only industry-wide method employed now is to rub one's finger across the back of the check -- if you can feel the embossment, then its too severe. Notwithstanding the finger-rub method, this lack of validity has led to a circle of finger pointing as bankers complain about their high reader/sorter reject rates to machine vendors who then blame the lack of MICR quality from the check printers, who in turn say that the majority of the problem comes from the bank's own encoding operations.

While the further outlook for the resolution of reader/sorter rejects is optimistic, there are nevertheless some options available for tackling this problem. These options range from monitoring reasons for the reader/sorter rejects to the design of measurement tests and related equipment.

The most direct and the most difficult way to solve the problem would be to develop a measurement device that could achieve the 1/1000 inch tolerance level now specified. Such a device would have to be inexpensive, accurate, repeatable and practical to use at the bank's and check printer's MICR operations.

Measurement of Strength or Internal Bonding of Paper

Another concern of the banking industry is the quality of the paper that is used for checks. Currently under the direction of ANSI X9 Financial Services

Committee and chaired by Mr. Gilbert Arbuckle, there is a voluntary group of financial executives who are developing specification standards for checks. The committee will attempt to provide assurances that checks will be able to withstand the degree of individual and automated handling that is used in check processing, especially as the equipment used to encode and process checks develops greater speed and sophistication. Specifications that will be looked at include weight, grain direction, porosity, stiffness, tearing, reflectance coatings and continuous form. Particular attention will be given to the minimum requirements for reader/sorter machines. The check specifications could be finished in about a year. Once they are approved as ANSI standards, banks and the Federal Reserve could then demand the standards from check manufacturers.

Measurement standards concerning paper are under the control of the Trade Association for Paper and Pulp Industry (TAPPI). In some cases, more than one method can be used to measure a paper characteristic. Under these circumstances, assistance could be used by the ANSI committee in determining which method would be best.

The problem is that there are no acceptable tests for strength or internal bonding characteristics of paper. As checks go through the reader/sorter machines, they travel at approximately 35 mph and have two counteractive forces acting upon them -- one pulling forward and one restraining. Under these conditions, a paper's internal bonding quality is important so that the paper's fibers do not separate. This fiber separation in combination with severe embossment are responsible for the reader/sorter rejects, with fiber separation being the lesser cause.

The test now used for internal bonding is the wax-pick test. Under this method, an internal bonding value is arrived at by having special grades of hot wax placed and pulled off paper until fibers start to be picked up by the wax. This test was shown to be ineffective in meeting the industry's accuracy requirements, when in analyzing a flurry of rejects that were happening to IBM reader/sorter machines a couple of years ago, there was found to be no correlation between a check's internal bond value and its chance of being a reject.

Problems and Opportunities in Optical Character Recognition (OCR)

Banking was the leading sector for the OCR market in 1982. According to International Resource Development,[1] banks led with $120 million in sales out

[1] "Machines that Read Move Up A Grade". High Technology. February 1983, p. 40.

of the total OCR market of $350 million. OCR is currently used in the banking industry primarily for the repair function of the MICR line. Recent developments may make it likely that an expanded use of OCR will be in banking's future.

One use of OCR could be to read the number that a person writes in for the dollar amount of the check. Just such a system was tested by IBM a couple of years ago. The test did not prove to be effective as the accuracy level was approximately 60 percent, too low a rate to justify the cost. The problem, however, was not in the OCR technology as much as it was with the checks themselves. Graphics were to be found all over the face of a check which caused the OCR system to be unable to clearly distinguish and locate the dollar amount. The check problem has now been solved by the industry with the "Bank Check Standard Background and Numerical Convenience Amount Field" (ANSI X9.7-1981). This standard has cleaned up the graphics on checks and designated a white background for the check amount location.

The use of OCR for reading the check amount should lead to gains in productivity and system performance for banks. An automated OCR system would replace the current labor-intensive encoding operation that consumes the largest amount of labor time and has the second lowest productivity level of the check processing operations.

Work is now proceeding on the use of OCR to read bar codes that would be placed on the back of checks -- similar to the bar codes on grocery items that are read at the supermarkets. Bar codes would identify the bank of first deposit, reduce rejects and misreads, and further automate the handling and sorting of checks.

Banking's increase use of bulk filing should provide for economies of scale incentives for OCR use. Bulk filing is a method of storing processed checks in one central location instead of sending them immediately to the individual banks. The increased check processing activity at one central location would make the cost of an OCR system more justified. Recognition Equipment has introduced an OCR system that serves bulk filing's purpose. Their system reads the MICR information, takes a digital image of the check, and uses the recognized MICR information to sort the images. The bank's monthly statement to the customer contains images of the checks -- not the checks themselves -- reduced in size to fit on a few pages.

The expanded use of OCR technology in banking will depend upon the banking industry reaching a collective agreement on what direction will be their overall

automation plans in the future. This consensus is necessary if the vendors are to provide the technology. At a roundtable discussion by check experts on the future of the check payment system, the view was expressed that OCR technology would be further along if the signal was clearer from the banking industry five years ago.[1]

WHOLESALE ELECTRONIC FUNDS TRANSFER

Wholesale EFT is composed of four principle commercial funds transfer networks -- FedWire, BankWire/CashWire, The Clearing House for Interbank Payments Systems (CHIPS), and Society for Worldwide Interbank Financial Telecommunications (SWIFT). The impetus behind the development of these payment mechanisms is geared towards minimizing the need for handling paper instruments, speeding up the transfer of ownership of funds, reducing the cost of operating the payment mechanism, and increasing the reliability of the system.

The growth rate of transfers sent through the four networks have been growing rapidly. Daily dollar values of corporate and correspondent payments have increased from $16 billion a day, in the early sixties, to over $600 billion a day in 1982. This translates into a doubling of volume every four years since 1960. The growth rate of transfer volumes should continue at approximately 15 percent a year over the next three years with the dollar amount increasing at a faster rate than either the volume rate or inflation.[2]

Automation Status

The automated integration of fund transfer systems by commercial banks is on the rise. In 1982, 23 percent had integrated wire systems with 44 percent planning to change over during the next three years. In addition, an increasing proportion of banks without integrated systems are converting from manual to automated operations.

---

[1] "Checks in Transition: Why and How Fast". ABA Banking Journal. June 1982, p. 47.

[2] "Time for the Industry to Improve Efficiency of Wire TRansfers". ABA Banking Journal. April 1983, p. 58.

Problems and Barriers to Growth

A survey of use of EFT by commercial banks conducted by the Bank Administration Institute (BAI), revealed that the most important concerns of management are message security and lack of uniform standards throughout the industry. Sixty-six percent of respondents were concerned about lack of industry standards, followed by security, which was mentioned by 61 percent of the respondents. The two concerns are interrelated since a lack of uniform standards force the banks to relax controls in order to meet the competitive pressures of customer service.

The BAI survey found that encryption techniques were used by 11 percent of the banks, with the majority of encryption being used over the SWIFT network. Much of the security concerns uncovered in the survey refer to manual procedures and policies rather than complex technical issues, such as data encryption. Thus, rapid improvements of controls could occur if uniform standards and procedures were agreed upon by the banking industry. The survey found that 46 percent of the funds transfer agreements do not limit transfer amount; 48 percent do not specify time deadlines; liability for compensation is specifically covered in 41 percent of the agreements; only ten percent would refuse to accept a funds transfer not covered by an agreement from an existing customer and only 24 percent would refuse the transfer request from a new customer.[1]

Efforts for funds transfer agreements are hampered by the lack of applicable laws, definition of common banking practice and forum to voice procedural concerns.

Transfers involving only one of the four networks seldom cause banks much problem. The problems arise when they must handle transfers that involve more than one network or when a transfer requires additional information that cannot be accommodated by a network's format. These situations can lead to inefficient and costly operating procedures for banks, including exception processing, frequent delays, exposure to loss, customer dissatisfaction and compensation claims.

The banks in the BAI survey reported a dramatic 360 percent increase in compensation claims for damages resulting from network malfunctions. Sixty-three claims were reported during the three years before 1981 and 114 were reported from 1981 to June, 1982.

---

[1]Bank Administration Institute. Studies in Funds Transfer. Rolling Meadows, Illinois, 1982, p. 16.

Banks have been developing automated systems to bridge the incompatibility of the wire networks. The ABA has published a set of guidelines for network format conventions and conversion rules in order to help banks automate their funds transfer process.

Some within the industry have questioned the appropriateness of keeping four discrete networks.[1] Originally each of the networks were created to serve a specific purpose and select constituency. Over time, however, a significant number of banks became active users of all four systems. The result has been a fragmented, inefficient system. A study by Arthur D. Little[2] of the payment system observed that activities proceed component by component. The resulting competition among the various payment networks does not insure or encourage coordination and may lead to inefficient use of resources. Suggestions to unify the wire transfers include combining BankWire and CHIPS, and setting up a nationwide settlement feature within SWIFT. The Steering Committee of the SWIFT U.S. National Group has requested that the Association of Reserve City Bankers look further into the subject.

RETAIL ELECTRONIC FUNDS TRANSFER

The last few years have witnessed the emergence and adoption of technological solutions to the payments problem. These technological changes involve the beginning deployment of automated teller machines (ATMs), the development of shared ATM networks, and point-of-sale (POS) systems, which are the next steps in the ladder of solutions to the retail payment system.

Automated Teller Machines

ATMs offer an alternative to the check for acquiring cash. ATMs are the most popular EFT service and account for 70 percent of all EFT transactions. Over 9,000 banks have installed ATMs. In 1983, ATMs accounted for 3.75 billion financial transactions totalling $105 billion in ATM withdrawals and $214

---

[1]Quoted in Donald R. Hollis. "Time For the Industry to Improve Efficiency Transfers". ABA Banking Journal. April 1983, p. 58.

[2]Ibid.

billion in ATM deposits.[1] An IBM study on bank automation found that by 1986, off-line teller transactions will cost 82 cents, on-line teller transactions will cost 48 cents, and ATM transactions will cost 28 cents.[2] Table S-2 shows the rapid increase in the number of ATMs over the last couple of years with a projection of over 100,000 machines by 1990.

Table S-2

AUTOMATED TELLER MACHINES IN OPERATION -- 1980-1990

1980	1982	1983	1990
10,000	32,000	47,000	125,000

Source: Robert M. Garsson "Easy Money". Datamation. January, 1984, p. 33.

Shared ATMs

Similar to the growth and popularity of ATMs, have been the proliferation of ATM networks. Forty percent of the ATMs are linked to one of the 150 regional or seven national shared EFT networks. Interfacing to a national network can be a technical burden that may require months to do at a cost of $10,000 - $30,000.

About one-half of the nation's networks have the capacity to support POS payments as well as ATM transactions. Those that do not, will have to replace their switch if they want to process POS payments. Roger J. Abouchar, Division Vice President of Anacomp, predicts that 500 additional switches will be installed by 1990 at a cost of $300,000 to $500,000 each.[3] Table S-3 shows some characteristics of the nationwide EFT retail networks. Probably the most important aspect of the shared networks is the number of shared debit cards. Bank Network News estimates that there are now over 50 million shared ATM access

---

[1]Linda Fenner Zimmer. "ATMs 1983". Bank Administration. May 1984, p. 25.

[2]Quoted in Ahmed S. Zaki. "Regulation of Electronic Funds Transfer: Impact and Legal Issues". Communications of the ACM. February 1983, p. 116.

[3]Robert M.Garsson. "Easy Money". Datamation. January 1984, p. 34.

Table S-3: NATIONAL EFT RETAIL NETWORKS

Network	Terminals	Card Base	Cost	Membership Composition
CIRRUS Oak Brook, IL	3,500 in 34 states	11 million	initiation fee plus $.75 per withdrawal and $.50 per inquiry; network keeps $.25.	12 owners and 600 sponsored members
EXPRESS CASH New York, NY	1,011 in 16 states	2 million	no initiation fee; transaction fee $1; network keeps $.50.	900 financial institutions
THE EXCHANGE Clifton, NY	2,500 in 35 states	3 million	not available	583 mostly smaller financial institutions.
PLUS SYSTEM Denver, CO	2,200 in 47 states	19 million	proprietary members pay a $200,000 initial fee, $.75 transaction fee; network keeps $.25; sponsored members pay $500 initial fee.	34 proprietary members and 1,100 sponsored members; 10% are savings associations
MASTER TELLER New York, NY	1,500 in 24 states	not available	no initiation fee; $1.64 transaction fee transmitted to ATM owner.	160 financial institutions
NATIONET Brown Deer, WI	5,000 in 26 states	expected 20 million	$5,000 stock purchase plus $25,000 initiation fee; transaction fee $.70; network keeps $.15.	13 network members
VISA San Francisco, CA	50 now, 6,000 committed worldwide; 3,800 committed in U.S.	expected 30 million	not available	230 banks

Source: "ATM Networks Span the Nation". Savings and Loan News. April 1983, p. 51 and "National Networks Postpone a Shakeout". Bank Network News. December 16, 1983, p. 2.

cards, up from 29 million last year. The shared debit card base will help bring about the next and larger phase of retail EFT -- direct debits at the point-of-sale (POS). Every national network and many regional networks are initiating POS projects or looking at it for the future.

Point-of-Sale

POS terminal systems have been getting cheaper, more reliable, and easier to service. The terminals of the past were teller terminals installed in merchant locations. They were expensive and difficult to use in a retail environment. Their cost dictated that only one or two could be used in a retail store.

Diebold has come out with a modular system that can drive up to 60 terminals and eight dedicated communications lines. It can be hooked up to ATMs, teller terminals, POS terminals, energy management systems, electronic security devices and automated fuel systems, and only cost $20,000. NCR has developed a modular ATM/POS terminal for the retail environment. It can handle four currency denominations, can handle deposits, and reads all three tracks on magnetic cards. It sells for $15,000 - $20,000 per machine. NCR is also marketing a product line of self-service terminals which will sell gasoline, airline, theatre, and ski lift tickets.

The cost of a POS transaction is already lower than the cost of a paper-based transaction. Currently, POS systems charge transaction fees of about 20 cents compared to 45 cents for the cost of a paper-based transaction.[1] The cost advantage is expected to increase over time. Electronic POS is not labor- and transportation-intensive, but relies on intensive use of computer and telecommunication systems which have been declining in cost.

As opposed to ATMs which started out as proprietary networks, POS will start out as shared networks. To make POS economically feasible, a critical mass (some say 75 percent of debit cardholders) will have to be able to access the retailers POS system. Shared ATM networks are bringing about this realization. There are now 50 million ATM shared network cards compared to 29 million in 1982. This represents 67 percent of all debit cards in the United States.

No matter how attractive EFT is for merchants and financial institutions and how much the technology progresses, POS will ultimately depend upon consumer

---

[1] "In-Store ATMs: Stepping Stone to POS". Federal Reserve Bank of Atlanta Economic Review. January 1984, p. 41

acceptance. Presently, consumers perceive debit cards as just another way to do something that checks, cash, and credit cards already do. Consumers may even perceive debit cards as being inferior to traditional payment methods as they lose float and control of stop payment orders. Only when consumers begin seeing an economic advantage will they begin to adopt debit cards. The perception of debit cards should become more appreciative as financial institutions and merchants begin pricing the payment methods at their true cost. In addition, consumers will start realizing the other benefits of debit cards such as time and place convenience, need to carry less cash, and quicker checkout times.

Consumer acceptance of debit cards will also be helped by the large majority who already carry ATM cards and are familiar with using transaction terminals and PINs. Retail stores who install ATMs will also help condition the consumers to the transition to POS.

The Federal Bank of Atlanta sees the second step of electronic POS payments taking place between 1985 and 1989. They predict that by 1987, debit cards will account for 15 percent of all retail purchases out of checking accounts.[1]

Barriers to Adoption And Use of Technologies

The next five years will witness the rapid growth of ATMs and the initial period of deployment of POS terminals. This growth period is anticipated in view of a convergence of economic and technological factors. The only clouds in the horizon concern the lack of compliance with communication protocols in the ATM networks and the security problems concerning EFT transactions.

Economic and Technical Aspects

The economic factors in the use of ATM machines by the banking sector and retailers are favorable. The costs to the banks per ATM transaction is 40 percent less than the cost per on-line letter transaction and 65 percent less than the cost per off-line teller transactions.[2] The consumer is able to save the bank charges for checks processed and, in addition, to save time spent in transactions with tellers.

---

[1] "Displacing the Check". Federal Reserve Bank of Atlanta Economic Review. August 1983, p. 41.

[2] Ahmed S. Zaki. Op. Cit.

The same is true of the deployment of POS terminals with their cost and time savings for retailers, banks, and consumers.[1] Technological changes have brought down the cost of POS terminals which now are more reliable and easier to service. While the growth of shared ATM networks has contributed to gaining the critical mass of cardholders needed for the economic feasibility of POS systems, in the end this feasibility will depend on consumer acceptance. However, given the expected future increases in bank charges for processing checks, consumer acceptance may be realized faster than many realize. By the early 1990s there will be a huge mass of households experienced with ATM cards, making the transition to POS easier.

Standards and ATM Networks

Industry-wide standards are needed for EFT and are just beginning to be tackled by the ATM networks. The first meeting of the EFT Network Council, a committee to develop standards, was held on June 5, 1984 in Washington, D.C. At an ANSI X9A meeting on April 19, 1984, David O'Connor, Chairman of the newly formed standards committee, claimed that at a meeting of representatives of seven national and regional ATM networks, the participants were not aware of ANSI standards. The first meeting on June 5th determined how the committee would relate to ANSI, ABA and International Standards Organization (ISO) efforts to help solve the immediate problem of network interface. This is an area that needs industry attention to ensure that different ATM networks can connect. If permitted to grow without attention to communications protocol standards, a barrier to rapid growth of shared ATM networks and POS transactions will be created.

Security

The security of EFT transactions poses threats to its growth. The security problem, because of its complexity and importance, is discussed next in more detail.

---

[1] "In-Store ATMs: Stepping Stone to POS". Federal Reserve Bank of Atlanta Economic Review. January 1984, p. 41.

The rising use and dollar amount of wholesale and retail EFT has led to a parallel increase in concern about the security of these systems. Security in electronic payment systems are comprised of two distinct aspects -- operational reliability and vulnerability to deliberate tampering.

Components of EFT systems that are vulnerable to tampering include terminals, communications links, and computers. Security precautions to avoid terminal vulnerability include using passwords, data encryption, fingerprints, voiceprints, and signature verification. Message authentication is increasingly used as a safeguard for active wiretapping as well as transmission and operator errors. Cryptography and computer software such as the Cobol Missing Branch Indicator (COMBI) are used to protect information stored on computers.

Barriers to The Adoption And Use of Security Technologies

The most important of the emerging banking security technologies concern data encryption. Encryption in the United States relies primarily upon the Data Encryption Standard (DES) algorithm, developed by the National Bureau of Standards. This section describes the data encryption standard and the barriers to its adoption.

Applicable Technical Standards

The ANSI Committee X9E8 on Financial Services has adopted a message authentication method, based on the DES algorithm, entitled Financial Institution Message Authentication (FIMA) X9.9. The DES is based upon an algorithm submitted by IBM and is also a Federal Information Processing Standard. [1]

The message authentication process provides security against active wiretapping and transmission/operator errors. The authentication process includes the computation, transmission, and validation of a Message Authentication Code (MAC). The DES, which requires a secret key, is used to generate the MAC. The MAC can either be used on the complete message or on a select part. The MAC is added to the message by the sender. The message is accepted as authentic by

---

[1]American National Standard for Financial Institution Message Authentication, American Bankers Association, Washington, D.C., April 13, 1982, p. 4.

the receiver if the same algorithm and secret key produce identical MACs. The equipment to perform data authenticity can cost from $2,000 to $3,000 per unit and each terminal site would have to have such a unit. Research conducted by SRI International's Computer Security Group indicates that generally, encryption is the only cost-effective way to counter certain threats to information and communication systems.[1]

Barriers to The Use of Encryption

Encryption must be used in the financial community in the transmission and storage of a person's PIN. Such environments include ATM and POS activities. Currently, only the PIN is encrypted and not the entire message. This is due to the encryption process being relatively slow. It takes approximately one second to encrypt ten characters. A typical ATM transaction has about 300 characters which would take too long to encrypt. Encryption is made more complex as networks link together. Encryption requires security modules at the various switching points and also requires that an ATM be able to encrypt a person's PIN. Not all ATM's installed have this capability. A retrofit encryption package costs about $1,000 from the major ATM manufacturers.

The road blocks to the use of encryption are two-fold: level of perceived threat and economics. Banks have not been using encryption because there have been very few cases of known wiretapping. SRI International maintains a listing of computer abuses. There were only two cases of reported wiretappping in over 700 incidents.[2]

The cost of encryption is also an important barrier to growth. The major elements of cost associated with cryptography are:

- purchase price of the hardware;
- system delays imposed by the use of cryptography; (software for cryption typically involves unacceptable transformation delays);
- training for users, system maintainers, system designers, and others involved with the system;
- key distribution and management;

---

[1]Quoted in: Charles Cresson Wood, "Future Applications of Cryptography". Journal of Telecommunication Networks. Summer 1982, p. 66.

[2]Ibid.

An encrypted communications link requires a DES device at both link ends. One encryption device is at the host computer and a similar device is at each terminal used to access the host computer. Add-on DES devices can cost between $2,000 and $3,500 per terminal with an average price of $2,200 without such options as special key management features. In addition to the cost of the DES equipment, the management of the keys can be an added and difficult burden. The future of cryptography lies in building the DES into the equipment at the start. The cost would then be less than $100 per terminal for DES security.

Given the higher costs associated with encryption, it is likely that lower level inexpensive security control will first be implemented previous to encryption.[1]

Regulatory and Legislative Pressures

Encryption may soon be warranted in many systems not so much because it is indicated by its economics, but because it will be mandated by a standard of due care. The Foreign Corrupt Practices Act of 1977 legislated that management may be held liable for negligence for failing to install the appropriate communications control measures. The Privacy Act of 1974 and the Office of Management and Budget Directive A-71 have similarly attempted to create a standard of due care for Federal government information and communications systems. Encryption may also be mandated in the banking community by legislation. A draft is before the Secretary of the Treasuary, Mr. Donald T. Regan, that would require encryption to be used in certain situations.

Industry Perceptions

Conversations with banking industry officials revealed the key role played by the Bureau in the development of encryption standards. The Chairman of the ANSI Committee X9E8, Mr. Blake Greenlee of Citibank, claimed that the Bureau's work with the financial community in developing security and encryption standards had been responsible for the promulgation of a higher quality standard as

[1]Some of these other security control devices include multiplexing of transmission lines, use of synchronous data streams, use of the highest possible transmission speeds, use of block transmission, use of advanced line protocols, etc.

well as ensured compatibility between the standards in use in the private sector and those public sector standards used by the Federal Reserve Board and the U.S. Treasury Department.

Mr. Greenlee also conveyed the industry perceptions of the need for an even greater effort on the part of NBS. These perceptions included the need for NBS to:

- speed the development of security standards as there are currently only a handful of people working on all the standards development;
- serve as a testing facility where equipment manufacturers could bring their security equipment to ensure that their equipment complies with the standards. NBS would not endorse their equipment, only provide the testing facilities;
- help develop processing and information standards that would be as important in the service industries as the initial NBS efforts in length, time, and weight were to the manufacturing industries;

In spite of the barriers mentioned earlier, the future outlook for encryption uses is good. As banking operations become more automated, DES will be built into equipment as systems begin to emphasize end-to-end rather than link-to-link encryption for better security.

SMART CARD

The smart card or (carte a memoire) has been pioneered in France by a combined effort of the government and private firms. The smart card is basically a credit card implanted with an integrated circuit chip or chips with non-volatile memory and computational capabilities. Present commercially available cards hold up to 12 kilobytes of information. Cards must be replaced after their memories are completely filled. The computational capabilities of the microprocessor are used to execute algorithms, such as personal identification number (PIN) comparisons, message authentication and data encryption operations, to control the use of the memory, and as an electronic authorization and payments method.

Uses

The smart card was originially conceived as being used in a debit POS system. The French believe that the smart card will replace current payment methods because it offers security against theft and fraud, avoids high transaction costs and provides greater flexibility in use. In a POS system, the issuing bank will personalize the card with the customer's account number, PIN and secret bank code word. The bank will also establish a monthly spending limit that can be programmed into each card and automatically reset each month.

The most important application of the smart card may be for security. Smart cards can have security features that only a computing device could have. Magnetic-stripe and digital optical cards can be made components of security systems, but they cannot have the full security of a device that can execute programming instructions internally. The security functions that can be performed by smart cards are: identification of bearer, encryption or deciphering of messages, protection against forged cards, authentication of transactions involving the card, and protection of records stored in the card. Smart cards are also used to store health and financial transaction data.

Barriers to Adoption and Use

While a major push in smart card activity is going on in France, where a combination of private and public efforts have developed and promoted its application, the American efforts languish in comparison. In France, the Ministry of Postes, Telephones et Telegraph will issue 1.5 million multiservice smart cards during 1984 to be used in banking, videotex, telephone, and television decoding operations. In the United States, studies and tests of smart cards, have been conducted by the Departments of Defense and Agriculture and by selected financial institutions such as Bank of America, First Bank of Minneapolis, Chemical Bank, Citicorp, American Express, and Chase Manhattan Bank, among others.

Adoption of the smart card will not come as easily to the United States as in France. The government and banking cooperation that helps to ensure uniformity and acceptance of the technology in France will be difficult to replicate in the U.S. The two major barriers to the smart card are the cost of the card itself and the infrastructure necessary for it.

The cost of the smart card is becoming less of a barrier. In 1982, cards were priced at $11 in batches over 10,000. They now are priced at $2 to $10, and depending upon the card's capabilities and quantities manufactured, prices should continue to decline in the future.

Meanwhile, the cost of standard magnetic cards (presently, about $.75) are rising due to the extra security measures being added to the card, including hologram insignias, microprinting and graphics visible only under ultraviolet light. These security devices are needed as credit card fraud is dramatically rising. The smart card's increasingly low price and the potential savings in fraud loss through its enhanced security features will make it more economically attractive in the future.

The infrastructure already in place in the financial community is based on magnetic stripe technology and will not disappear in the foreseeable future because of the enormous investments associated with it. Thus, any new technology must be compatible with magnetic stripe technology and slowly replace it over time. The smart card meets this criterion as it is compatible with magnetic stripe technology. France's two leading credit card companies will introduce just such a smart card combined with magnetic stripes. The so called "smart stripe card" will allow the smart card to be introduced without abandoning the huge investment in magnetic stripe technology. There are specialized areas where banks could immediately use the smart card. These include high dollar money transfers and home banking situations.

Most experts monitoring smart card developments think that banking will not be the first U.S. user of the technology but that adoption will first come in closed-end situations where the card will fulfill needs not presently met. One such area is the medical field where a smart card could authenticate claims and carry personal medical histories.

Standards Activities And Technical Support Needs

To expedite progress in standards, a multinational organization called International Association for Microcircuit Cards (INTAMIC) was established in France in June 1981. Its members include banks and other financial institutions from several European countries, the Far East and the United States, including Chase Manhattan Bank and Bank of America. INTAMIC has taken over most of the conceptual and technical development functions of the smart card. Using INTAMIC

and other government's inputs, the ISO has developed a draft standard for the physical interface, and a draft proposal on data interchange between cards and readers. The smart card meets ISO specifications, having the same size, flexing capabilities, survival over a wide range of temperatures and humidity, and thickness, of ordinary plastic credit cards. Smart cards are also compatible with embossing and magnetic stripes to ensure duality of use for presently magnetic stripe-based operations.

In the United States, the American National Standards Institute (ANSI) X3B10.1 committee will handle the physical and technical issues of the smart card and act as a liaison to ISO. Once smart card standards are determined, there will be a need for a test facility run by an impartial third party to determine if manufacturer's cards meet the specified standards. NBS could provide such a service, which would be comparable to the magnetic tape comparison that NBS provides for credit cards.

HOME BANKING

Home banking systems have generally received the most favorable reviews of all videotex services among consumers. Home banking is attractive to customers as it can provide both cost and convenience benefits for their existing banking needs and can offer services which were unavailable before. These services include balance inquiries, credit card account status, automatic payments, bill payments, funds transfer, stop payments, and account maintenance operations.

Pilot Tests and Services

As many as 12 pilot tests of home banking operations have been conducted during the last four years. Some of these pilot tests have progressed to commercial operations. The most important of the services are Pronto Home Banking (owned by the Chemical Bank) which has 2,000 customers, the Viewtron project in Coral Gables (Florida) which serves 5,000 households, Home Bank Interchange, a joint venture of 25-30 banks, and ADP Telephone Computing Services which is serving 5,000 customers in various locations.

Market Potential

Projections of the growth of the home banking market are presented in Table S-4. Home banking projections are closely tied to the growth of the home computer industry, because of the relatively high costs of terminal equipment to the consumer. Home banking revenues are projected to $850 million in 1995, not an inconsequential market.

Table S-4

HOME BANKING MARKET PROJECTION

	1987	1995
Percent Households With Videotex	6.0%	20.0%
Home Banking Revenues (million $)	$85	$850
Percent of Total Videotex Revenues	8.5%	14.0%
Revenue Per Month Per Customer	$1.26	$3.75

Source: Predicast Inc. U.S. Videotex and Teletext Markets. Cleveland, Ohio, 1983, p. 64.

Another market projection of home banking was provided by a year-long study conducted by the Bank Administration Institute and Arthur Anderson and Company[1] study which surveyed hundreds of banking and financial service leaders. The consensus was that home banking will be offered by fewer than 20 percent of commercial banks by 1986 and probably will not be profitable by 1990. Bank panelists predicted that five percent of households would utilize home banking in 1986, increasing to 11 percent in 1990.

Barriers To Growth

A number of problems and barriers to the growth of home banking services are noted. Some of these barriers are economic in nature, others involve legal and privacy problems.

---

[1]Katherine L. George. "Savings Institutions Begin to Test Electronic Waters of Home Banking". Magazine of Bank Administration. January 1984, p. 30.

Costs of Bank Participation

It appears that home banking operations, requiring investments close to $7 - $10 million will only be marginally profitable at least in the short run. A study of the economics of home banking conducted by Communications Studies and Planning (CSP) International[1] concluded that the banks will require between 13,000 and 52,000 video banking customers to break even, depending on whether they purchase software and processing services from third parties or develop them in-house. CSP International concluded that home banking will be only marginally profitable at best for the next five years. CSP feels the increasing use of home computers and other videotex services will have a significant beneficiary impact on home banking. The study stressed that while only marginally profitable, other factors such as potential cost-savings and inter bank competition will be incentives for home banking.

Costs to the Consumer

The main barrier to the consumer will be the equipment related costs of videotex. At present, videotex terminals of limited graphic capabilities are being offered at $500-$600 per unit in some commercial videotex services. In some videotex options the consumer will have to purchase decoders ($600), modems ($200), and printers ($200-$300). Because of these significant costs to the consumer, the growth of home banking services via videotex will be dependent on the growth of home computers. Those consumers with home computers will become the obvious clients of home banking services.

Liability Privacy and Security Problems

A policy issue that will have to be decided is who will have the responsibility for a transaction. If a transaction is lost or unauthorized, will the service provider, system operator, network provider, credit provider or end user be liable for it. Under the existing EFT Act, a bank will bear most of the losses from an unauthorized transaction unless it can prove the transaction was

[1]"Are Banks Really Ready for Video Banking". ABA Banking Journal. December, 1983, p. 79.

authorized. To protect against such losses, audit trails will be particularly important in video banking systems since the procedures are new and paperless.

Privacy and security would be made easier if only banks operated the system, offered only banking transactions, and used equipment dedicated exclusively to banking purposes. Thus, the operation would be covered by present fiduciary and legal duties. As videotex systems usually will involve many financial and non-financial organizations offering a variety of services, problems of security and privacy become more acute.

Currently, personal data are kept in separate organizations -- in banks, insurance companies, credit card accounts, retail stores. If a videotex system would unify these accounts, there will be great pressure to compile consumer financial profiles for marketing and credit decision purposes. The transmission network will have to be secure from electronic eavesdropping. The most vulnerable point will be between the home terminal and the first central office, i.e., the local loop.

1

STUDY OBJECTIVES AND BACKGROUND

This case study of technologies related to payment systems in the banking industry is part of a larger study of technological trends in the service sector. Other portions of the study deal with general and technological trends in the service sector of the U.S. economy and with the emerging videotex/teletext industry.

STUDY OBJECTIVES

The objectives of this case study of payment systems in the banking industry are:

1. to develop data and information on the growth prospects of payment technology in the banking sector;

2. to assess barriers -- economic and technological -- to the adoption and use of these technologies; and

3. to identify to the extent possible the work on standards and technological support required in view of the expected growth.

The payment and electronic fund transfers technologies were identified as candidates for a case study in an analysis of technological trends in the U.S. service sector. The study of technological trends presented in Volume I of this study identified the banking industry as having one of the highest rates

of growth among service sector industries. In addition, payment system technologies were found to have important implications for the service sectors which interact directly with the consumer, such as retailing, among others.

BANKING AND PAYMENT SYSTEMS

Few sectors of the economy have been subjected to more economic regulatory and technological changes as the banking sector has been exposed to during the last five to six years. In 1980, the Depository Institutions Deregulation and Monetary Control Act phased out all the legally imposed interest rate ceilings paid on deposits, opening up competition for short run cash management services between banks and other financial institutions. The late seventies witnessed the marketing of money market mutual funds by non-banking institutions, an event that ushered the competitive pressure on banking from other financial institutions. In addition to the above, there has been a concurrent pattern of liberalizations of state branch banking laws with a significant number of states adopting statewide banking.

Partly in response to this wave of competitive pressures, a series of new banking services have been introduced. NOW accounts, interest bearing demand deposit accounts, have made their appearance, while other services, such as bill-paying and pre-authorized payment services have increasingly been offered. All this adds to the need for efficient bank operation in this competitive environment.

Parallel to these developments in the regulatory arena, the banking industry was experiencing a period of significant growth. Indeed, as shown in Table 1-1, banking grew faster than the private sector of the U.S. economy during the period 1973-1981, a period also characterized by faster rates of productivity and employment growth than for the national economy.

Demand for banking services is also expected to continue to grow faster than the national economy during the next decade.[1] In particular, the demand for bank processing of transactions has been appreciably growing at five to six percent annually, creating upward pressures on banking industry costs and resources. The 1980 Act referred to above enabled banks to "unbundle" the charges for the processing of checks and other banking services, enabling a

[1]See U. S. Department of Labor, Bureau of Labor Statistics. Economic Projections to 1990. Bulletin 2121, March 1982.

more rational approach to coping with the payment explosion and creating incentives for the adoption of technological changes that would enable handling of transactions in a more cost-effective manner.

Table 1-1

SELECTED GROWTH INDICATORS OF THE BANKING INDUSTRY -- 1973-1981

	Average Annual Rates of Changes			
	Real Output	Total Employment	Total Hours	Real Output per Hour
All Private Sectors	2.8%	2.4%	2.0%	0.8%
Banking	5.6%	4.1%	4.0%	1.6%

Source: Printouts from the U.S. Bureau of Labor Statistics. See also the publication: U.S. Department of Labor, Bureau of Labor Statistics. Time Series Data for Input - Output Industries. Bulletin No. 2018. U.S. Government Printing Office, 1979.

New technologies are being adopted by banks at increasing rates to cope with the explosion in payment services and transactions. These technologies are discussed in this report. Technologies and improvements in the processing of checks are discussed in Chapter 2, followed in Chapter 3 and Chapter 4 by electronic fund transfers. Security problems and related technologies are the subject of Chapter 5. Chapter 6 discusses the Smart Card, a promising new development, followed in Chapter 7 by home banking.

2

CHECK PROCESSING

BACKGROUND

The checkless society that had been predicted in the 1960's has yet to materialize. In fact, the number of checks has been steadily increasing, albeit at a slower rate in recent years. Some 35 billion checks are processed in a year, or about 100 million checks a day. Each check is processed by an average of 2.4 institutions.

The Federal Reserve Bank of Atlanta Check Study of 1979 found that the growth in the number of checks written averaged between five and six percent a year from 1974 through 1979.[1] Less clear is the growth rate today because it is no longer possible to directly count the number of checks. This is due to the greater number of institutions offering checkable deposits. There is a general consensus, however, that the rate of growth of checks is declining. What that rate is and how long it continues is very important since a four percent compound growth rate would result in a doubling of check volume in 12 years.

The latest study from the Atlanta Federal Reserve Bank's payment research team indicates that the total check volume should start to decrease within this decade.[2] They found that the growth in checks decelerated to a rate of about

---

[1]Quoted in "Displacing the Check". Federal Reserve Bank of Atlanta Economic Review. August 1983.

[2]Ibid. p. 2.

two percent a year from 1979-1984. Zero growth should occur by 1989 and a sharp decline of at least 25 percent should take place between 1989 and 1994.

In light of earlier reports which had predicted a higher growth rate in checks, the findings from the Atlanta bank's payment research team should come as a relief to the financial community whose check collection system is under strain.

Banking's check collection system is a loosely organized, yet coordinated system. There is no one central governing body which is responsible for the system's performance. Rather, the procedures for control, crediting, sorting, and security are partially controlled by the Federal Reserve System and the Uniform Commercial Code, and partially based on interbank agreements or clearinghouse arrangements. Each bank is responsible for its own processing operations and there are wide differences in the resources, productive capacity and quality that is found in the various commercial bank's check processing operations. Yet each bank would suffer if the system is not based upon cooperation and strict adherence to procedures from all members. While the system uses specialized check handling equipment, many suboperations are still labor-intensive.

The principal organizations that participate in the check collection network are commercial banks, clearinghouse associations and Federal Reserve Banks. The function of the check collection is to present checks as quickly as possible to the paying bank. Time is critical because checks in transit to paying banks represent opportunity cost (interest foregone while in transit) to the collecting bank or its customers. Thus, for large banks and Federal Reserve Bank facilities, check processing is a 24-hour operation.

The basis for the automation of check handling is the Magnetic Ink Character Recognition (MICR) line standard (ANSI X3.3-1970, revised in 1976). MICR encoding began appearing in 1958 arising out of a study conducted by the American Bankers Association (ABA). MICR encoding on the face of a check contains standard routing information, the amount of the check, the account number, and in-house codes.

The check handling operations are as follows. After the initial acceptance by a teller or mail room, the first operation is proofing. In the proofing operation all credits (deposit tickets) are balanced against their associated debits (checks) to prove that they are in balance. Concurrently, the bank of first deposit encodes the amount of the check in the lower right hand corner in magnetic ink characters that can be read by automated equipment.

The proofing-encoding operation requires an operator to read the check amount and key that value into a terminal. This is highly labor intensive and is estimated to require at least 45 million man-hours a year.

After completion of the proofing operation, checks are sorted by destination "on-us" checks and credits are sorted out for later processing, and "transit" checks are sorted into groups by collection path (e.g., to clearinghouse, to Federal Reserve Bank, to correspondent bank). Small banks perform the sorting operation by hand, while large banks use high-speed computer-driven electronic reader-sorter equipment.

Following the sorting operation, there is a further balancing-reconciliation operation to insure that the value being collected is equal to the value being credit. The transit checks are then dispatched for collection.

To measure the performance of the check collection system, the Bank Administration Institute has performed annual studies of the check collection systems of large commercial banks. Their latest findings for the year 1981 indicate that for the second consecutive year, improvements were made in the efficiency of most check collection operations.[1] They noted that technological support had never been better, but field engineering support is needed for the smooth operation of the check collection system.

PRODUCTIVITY IN CHECK PROCESSING OPERATIONS

As shown in Table 2-1, the overall total productivity for check processing tasks rose 5.1 percent in 1981 after remaining relatively stable during the previous two years. The average bank used approximately 1.0 less man-hours per 10,000 items processed. Productivity increases should continue as greater use is made of automated reject processing, bulk filing and check truncation, and as banking staff becomes more familiar with system operations. The productivity improvements noted, however, will only serve to maintain the status quo as check volume is expected to grow until 1990.

Because of the unbundling of Federal Reserve rates and charges for non-credit services, it is expected that the amount of encoded work for checks will increase due to price incentives. As Tables 2-2 and 2-3 indicate, the encoding

---

[1]Bank Administration Institute. 1981 Survey of the Check Collection System. Rolling Meadows, Illinois, 1982.

Table 2-1

LABOR PRODUCTIVITY IN CHECK PROCESSING OPERATIONS OF COMMERCIAL BANKS
1978-1981

(Average Checks Per Man-Hour)

Check Processing Operations	1978	1979	1980	1981
Balancing and Correction	2,559	2,456	2,880	3,218
Encoding Operations	928	859	865	876
• single-pocket machine	845	881	864	920
• multipocket machine	657	628	686	767
Check Receiving	N.A.	N.A.	6,519	8,970
Reader/Sorter Operations	12,423	12,527	11,740	13,044
Cash Letter Make-Up and Microfilming	7,262	6,261	6,323	6,215
• cash letter make-up	5,626	5,557	5,768	5,484
• microfilming	11,130	12,609	7,933	8,970
On-us Paying, Filing and Return Item Processing	831	1,066	965	824
Exception and Return Item Processing	26	34	27	24
• exception item processing	3	3	3	3
• return item processing	N.A.	85	54	48
Bulk Filing	N.A.	N.A.	N.A.	4,423
Reject Processing	297	309	308	248
Overall Labor Productivity	523	530	525	552

N.A. represents lack of comparable data availability.

Source: Bank Administration Institute. 1981 Survey of the Check Collection System. Rolling Meadows, Illinois, 1982, pp. 28-41.

Table 2-2

USE OF LABOR IN CHECK PROCESSING OPERATIONS OF COMMERCIAL BANKS
1978-1981

(man-hours)

Check Processing Operations	1978	1979	1980	1981
Balancing and Correction	4.1	3.5	3.5	3.1
Encoding Operations	5.5	5.7	5.0	5.2
Check Receiving	N.A.	N.A.	0.9	1.0
Reader/Sorter Operations	0.8	0.8	0.9	0.7
Cash Letter Make-Up and Microfilming	1.5	1.4	1.3	1.2
On-us Paying, Filing and Return Item Processing	5.8	5.3	4.3	3.9
Exception Item Processing	1.3	1.0	1.3	1.2
Bulk Filing	N.A.	N.A.	0.6	0.3
Miscellaneous	1.5	1.2	1.3	1.5
Total	20.5	18.9	19.1	18.1

N.A. represents lack of comparable data availability.

Source: Bank Administration Institute. 1981 Survey of the Check Collection System. Rolling Meadows, Illinois, 1982, p. 42.

Table 2-3

DISTRIBUTION OF LABOR IN CHECK PROCESSING OPERATIONS OF COMMERCIAL BANKS
1978-1981

(percent)

Check Processing Operations	1978	1979	1980	1981
Balancing and Correction	20.0%	18.4%	18.3%	17.2%
Encoding Operations	26.7	30.4	26.2	28.8
Check Receiving	N.A.	N.A.	4.5	5.7
Reader/Sorter Operations	3.9	4.2	4.5	4.0
Cash Letter Make-Up and Microfilming	7.4	7.5	6.9	6.8
On-us Paying, Filing and Return Item Processing	28.2	27.9	22.8	21.3
Exception Item Processing	6.3	6.6	6.6	6.5
Bulk Filing	N.A.	N.A.	3.2	1.6
Miscellaneous	7.5	5.0	7.0	8.1
	100.0%	100.0%	100.0%	100.0%

N.A. represents lack of comparable data availability.

Source: Bank Administration Institute. 1981 Survey of the Check Collection System. Rolling Meadows, Illinois, 1982, p. 30.

function is labor intensive and its operation consumes the largest percentage of labor. The upward trend in productivity should continue, however, as banks are implementing incentive plans for inscriber operators.

Return item productivity decreased in the period 1978-1981, and was down to 48 items per man-hour in 1981. Productivity levels should improve as automated systems are introduced and the ANSI X9.3-1981 check endorsement specification standard is adopted by the major clearing banks. The standard calls for a uniform placement of endorsement on the back of checks and will eliminate the confusing overlap of multiple endorsement stamps.

The productivity level for reject processing reflects the fact that most banks still process rejects by manual methods. As automated reject processing is used more, productivity levels should increase.

Transit holdover, shown in Table 2-4, is an important measure of a bank's processing efficiency because it reflects the speed that checks are collected.[1] Transit holdover refers to items that were received by a bank before a deadline but were not processed in time to be sent for collection. These items would result in a loss of float to a bank but not its customers. In 1981, the average transit holdover rate continued to decline to 1.4 percent. However, the dollar amount of the items increased, thus effectively cancelling some of the benefits from this improvement in productivity.

Table 2-4

CHARACTERISTICS OF CHECKS HELD IN TRANSIT

	1978	1979	1980	1981
Transit holdover as percent of total checks in transit	2.8%	2.5%	1.9%	1.4%
Average dollar value of check held over	$157	$661	$678	$781

Source: Bank Administration Institute. 1981 Survey of the Check Collection System. Rolling Meadows, Illinois, 1982, p. 24.

[1]Following banking terminology, checks sent to other banks for clearing purposes are labelled "transit" items, while checks cleared within the same bank are labelled "on-us" items.

Transit exception items are checks in transit that require special reconcilement with other banks. They may be composed of missent, miscoded, listing errors, free and lost items, etc., however, over 90 percent of them are return items. As shown in Table 2-5, the resolution time improved for outstanding exception items in 1981, and should continue in the future as software packages are developed by vendors to improve the productivity of the reconcilement operation. Transit return items (see Table 2-6) have been declining and stood at 910 for 100,000 items sent in 1981. Although the trend is improving, transit return items continue to be a significant and particularly costly exception item for bankers.

Table 2-5

CHARACTERISTICS OF TRANSIT EXCEPTION CHECKS (ITEMS)

	1978	1979	1980	1981
Transit exception items per 100,000 transit items processed	1,065	1,266	1,062	959
Percent of checks outstanding for more than one month	74.7%	70.1%	77.2%	70.9%

Source: Bank Administration Institute. 1981 Survey of the Check Collection System. Rolling Meadows, Illinois, 1982, p. 18.

Table 2-6

TRANSIT CHECK (ITEMS) RETURNS

(Rate per 100,000 of Transit Items Sent)

	1978	1979	1980	1981
Transit Check Returns	1,023	1,207	1,004	910

Source: Bank Administration Institute. 1981 Survey of the Check Collection System. Rolling Meadows, Illinois, 1982, p. 9.

The average cost of return items was found to be $0.29 in 1973 and $0.36 in 1981.[1] Improvements should be realized when automated systems and the check endorsement standard is widely adopted.

Table 2-7 and 2-8 shows statistics relating to the magnetic ink character recognition (MICR) line. The MICR line standard (ANSI X3.3 - 1970, revised in 1976) is the single most important standard concerning the processing of checks. The declining reader/sorter reject rates reflects the industry concern over MICR line quality control. A further reduction to 0.8 percent is achieved by some banks who have the capability of high-speed reentry of first pass rejects under software system control. An increasing number of banks have the capability of automated reject processing for reader/sorter rejects. The main features of an automated reject processing system include: machine stripping of the reject, optical character recognition (OCR) reading of the original MICR line, automated encoding of MICR data on the strip, and automated reentering of the MICR line information in the appropriate place in the captured data base. As shown in Table 2-8, banks are increasingly using their automated reject processing equipment (70.1% in 1981) rather than manual methods. There is still room for improvement however, as only 28 percent of the banks process all of their rejects by the automated method. A bank that does not utilize high-speed reentry or automated reject processing would probably use computer terminal operators to key the MICR line information through terminals. This method of on-line reject reentry has several disadvantages such as low productivity and human error.

BARRIERS TO FURTHER PRODUCTIVITY GAINS

Literature reviews and limited contacts with banking equipment manufacturers and banking industry officials revealed some issues of concern that may bar the path to productivity gains in check processing operations. Because these issues concern measurements and tests, of interest to NBS, they are discussed next.

Measurement of Embossment Levels of MICR Line

A current concern of the banking industry is the level of embossment of the MICR line, which is the primary cause of reader/sorter rejects. The MICR

[1]Bank Administration Institute. Op. Cit., p. 53.

Table 2-7

CHECK READER/SORTER REJECTION RATES
(percent)

	1978	1979	1980	1981
Check Rejection Rate	2.1%	2.1%	1.9%	1.7%
• transit routing number errors	19.5	19.2	18.6	15.1
• account number errors	16.1	18.5	15.7	16.3
• dollar amount errors	40.7	40.5	41.5	35.1
• serial number errors	N.A.	N.A.	N.A.	4.8
• trancode errors	N.A.	N.A.	N.A.	6.6
• other, unknown or multiple errors	23.7	21.9	24.2	22.1
Check Rejection Rate After High-Speed Reject Reentry	N.A.	N.A.	0.8%	0.8%

N.A. denotes information not available.

Source: Bank Administration Institute. 1981 Survey of the Check Collection System. Rolling Meadows, Illinois, 1982, pp. 6, 8, 44.

Table 2-8

AUTOMATED CHECK PROCESSING REJECTION RATES
(percent)

	1978	1979	1980	1981
Automated Check Processing Rejection Rates	66%	66.3%	68.6%	70.1%
Total Use of Automated Reject Processing	20%	15%	24%	28%

Source: Bank Administration Institute. 1981 Survey of the Check Collection System. Rolling Meadows, Illinois, 1982, pp. 48-40.

line problem can be caused by either the check printer who place part of the MICR information on a check, or by the bank's own MICR encoding, such as for the dollar amount. The current embossment depth standard is for a 1/1000 inch tolerance level. A too severe embossment will either lower the MICR signal level to an unreadable level or will cause a character to be read incorrectly.

There are no means today for printers or banks to measure their embossment level because there are no commercially available measurement devices to verify the 1/1000 inch tolerance level. In fact, the only industry-wide method employed now is to rub one's finger across the back of the check -- if you can feel the embossment, then its too severe. Notwithstanding the finger-rub method, this lack of validity has led to a circle of finger pointing as bankers complain about their high reader/sorter reject rates to machine vendors who then blame the lack of MICR quality from the check printers, who in turn say that the majority of the problem comes from the bank's own encoding operations.

While the further outlook for the resolution of reader/sorter rejects is optimistic, there are nevertheless some options available for tackling this problem. These options range from monitoring reasons for the reader/sorter rejects to the design of measurement tests and related equipment.

The most direct and the most difficult way to solve the problem would be to develop a measurement device that could achieve the 1/1000 inch tolerance level now specified. Such a device would have to be inexpensive, accurate, repeatable and practical to use at the bank's and check printer's MICR operations.

Monitoring the reasons for the rejection rates would entail conducting quantitative studies of the reasons for reader/sorter rejects. Answers would be sought for questions such as what is the critical point that rejects occur, and how is the reject rate distributed by the different characters (e.g., long vertical characters such as a "7" or a "1" have been thought to cause more rejects as the embossment is different at the top and bottom of the characters). This method would not directly solve the problem but would help to better understand and arrive at a solution.

The optimistic outlook for the resolution of the problem of reader/sorter rejects is based on the reduction in the check rejection rate from 1.7 percent to 0.8 percent when high-speed reject reentry is used, and on the increased use of automated reject processing rather than manual methods. In addition, over time there will be a move away from impact printing towards the use of offset printing which will not cause an embossment problem.

Measurement of Strength or Internal Bonding of Paper

Another concern of the banking industry is the quality of the paper that is used for checks. Currently under the direction of ANSI X9 Financial Services Committee and chaired by Mr. Gilbert Arbuckle, there is a voluntary group of financial executives who are developing specification standards for checks. The committee will attempt to provide assurances that checks will be able to withstand the degree of individual and automated handling that is used in check processing, especially as the equipment used to encode and process checks develops greater speed and sophistication. Specifications that will be looked at include weight, grain direction, porosity, stiffness, tearing, reflectance coatings and continuous form. Particular attention will be given to the minimum requirements for reader/sorter machines. The check specifications could be finished in about a year. Once they are approved as ANSI standards, banks and the Federal Reserve could then demand the standards from check manufacturers.

Measurement standards concerning paper are under the control of the Trade Association for Paper and Pulp Industry (TAPPI). In some cases, more than one method can be used to measure a paper characteristic. Under these circumstances, assistance could be used by the ANSI committee in determining which method would be best.

The problem is that there are no acceptable tests for strength or internal bonding characteristics of paper. As checks go through the reader/sorter machines, they travel at approximately 35 mph and have two counteractive forces acting upon them -- one pulling forward and one restraining. Under these conditions, a paper's internal bonding quality is important so that the paper's fibers do not separate. This fiber separation in combination with severe embossment are responsible for the reader/sorter rejects, with fiber separation being the lesser cause.

The test now used for internal bonding is the wax-pick test. Under this method, an internal bonding value is arrived at by having special grades of hot wax placed and pulled off paper until fibers start to be picked up by the wax. This test was shown to be ineffective in meeting the industry's accuracy requirements, when in analyzing a flurry of rejects that were happening to IBM reader/sorter machines a couple of years ago, there was found to be no correlation between a check's internal bond value and its chance of being a reject.

Banking was the leading sector for the OCR market in 1982, according to International Resource Development,[1] banks led with $120 million in sales out of the total OCR market of $350 million. Recognition Equipment, Inc. (Dallas) is the leading supplier of OCR equipment with nearly one-third of all OCR sales. Over two dozen other companies with OCR revenues under $20 million round out the industry, including Burroughs Office Systems Group (Danbury, CT) CompoScan (Fairfield, NJ), Dest (San Jose, CA), Hendrix Technologies (Manchester, NH), IBM (Charlotte, NC), Kurzweil Computer Products (Cambridge, MA) - a Xerox subsidiary, and NEC America (Melville, NY).

OCR is currently used in the banking industry primarily for the repair function of the MICR line. Recent developments may make it likely that an expanded use of OCR will be in banking's future.

One use of OCR could be to read the number that a person writes in for the dollar amount of the check. Just such a system was tested by IBM a couple of years ago. The test did not prove to be effective as the accuracy level was approximately 60 percent, too low a rate to justify the cost. The problem, however, was not in the OCR technology as much as it was with the checks themselves. Graphics were to be found all over the face of a check which caused the OCR system to be unable to clearly distinguish and locate the dollar amount. The check problem has now been solved by the industry with the "Bank Check Standard Background and Numerical Convenience Amount Field" (ANSI X9.7-1981). This standard has cleaned up the graphics on checks and designated a white background for the check amount location.

The use of OCR for reading the check amount should lead to gains in productivity and system performance for banks. An automated OCR system would replace the current labor-intensive encoding operation that consumes the largest amount of labor time and has the second lowest productivity level of the check processing operations.

Work is now proceeding on the use of OCR to read bar codes that would be placed on the back of checks -- similar to the bar codes on grocery items that are read at the supermarkets. Bar codes would identify the bank of first deposit, reduce rejects and misreads, and further automate the handling and sorting of checks.

---

[1]"Machines that Read Move Up A Grade". High Technology. February 1983, p. 40.

Banking's increase use of bulk filing should provide for economies of scale incentives for OCR use. Bulk filing is a method of storing processed checks in one central location instead of sending them immediately to the individual banks. The increased check processing activity at one central location would make the cost of an OCR system more justified. Recognition Equipment has introduced an OCR system that serves bulk filing's purpose. Their system reads the MICR information, takes a digital image of the check, and uses the recognized MICR information to sort the images. The bank's monthly statement to the customer contains images of the checks -- not the checks themselves -- reduced in size to fit on a few pages.

The expanded use of OCR technology in banking will depend upon the banking industry reaching a collective agreement on what direction will be their overall automation plans in the future. This consensus is necessary if the vendors are to provide the technology. At a roundtable discussion by check experts on the future of the check payment system, the view was expressed that OCR technology would be further along if the signal was clearer from the banking industry five years ago.[1]

Part of the uncertainty from the banking community stems from the varied and confusing roles that the Federal Reserve is supposed to perform. The Federal Reserve is supposed to 1) be a regulator, 2) ensure payment system efficiency, 3) be a clearer of last resort, 4) perform "public good" clearing, and 5) be a competitor as well by virtue of the Monetary Control Act of 1980. Charles Buchta, Vice President of The Chase Manhattan Bank expressed "because the Fed has been put in such an untenable -- and unpopular -- position, it's rather difficult for the financial industry to have a meaningful, cooperative discussion with the Fed on where we're going. Not only that, it's awfully hard to plan."[2]

The Monetary Control Act of 1980, which unbundled and increased the price of check processing by the Federal Reserve, has led to the banking's community uncertainty about their check processing operations. After Federal pricing, the volume of checks processed by the Federal Reserve fell by 20 percent. Banks saw this as an opportunity to increase their correspondent banking with some banks making large investments in systems and equipment for their check processing

---

[1]"Checks in Transition: Why and How Fast". ABA Banking Journal. June 1982, p. 47.

[2]Ibid. p. 47.

activities. Congress, however, with the same speed it enacted the Monetary Control Act can dis-enact it, leaving the banks holding the bag on their increased investments for check processing.

Roy Van Denburgh, planning representative from IBM's Systems Development and Product Support division, expressed the vendor industry views by saying "when I go back and try to tell the IBM company that it should spend $X million on the future of such and such technology, management is reluctant to do that because the banking industry hasn't really decided which way it wants to go. .... we've got to look into the future and predict we'll build X number of new machines at a certain price. We can't do that if the perspective changes."[1]

[1] Ibid. pp. 45, 47.

3

WHOLESALE ELECTRONIC FUNDS TRANSFER

BACKGROUND

Wholesale electronic funds transfer (EFT) is composed of four principle commercial funds transfer networks -- FedWire, BankWire/CashWire, The Clearing House for Interbank Payments Systems (CHIPS), and Society for Worldwide Interbank Financial Telecommunications (SWIFT). The impetus behind the development of these payment mechanisms is geared towards minimizing the need for handling paper instruments, speeding up the transfer of ownership of funds, reducing the cost of operating the payment mechanism, and increasing the reliability of the system. American banks have led the way in establishing these EFT systems for two main reasons: the dollar is the most cosmopolitan currency, and American firms have become nationwide and multinational, demanding that their banks follow suit.

SWIFT and BankWire are message-switching systems whereas FedWire, CHIPS and CashWire are funds transfer and settlement systems. A message-switching system only processes the message, conveying the identities of the payer and receiver. It is not a true payment system in that it does not establish an account relationship. This means that the exchange of value, the clearing and the settlement are delayed and performed separately. The distinction between a message-switching system and a payment system does not lie in the technology employed. A payment system just uses a much more powerful and advanced equipment and software as it has to perform more complex operations and must provide a higher level of security.

The growth rate of transfers sent through the four networks have been growing rapidly. Daily dollar values of corporate and correspondent payments have increased from $16 billion a day, in the early sixties, to over $600 billion a day in 1982. This translates into a doubling of volume every four years since 1960. The growth rate of transfer volumes should continue at approximately 15 percent a year over the next three years with the dollar amount increasing at a faster rate than either the volume rate or inflation.[1]

FedWire is an on-line communications network linking Federal Reserve offices and member banks nationwide. FedWire is the largest funds transfer system in the United States. Over 800 banks use it to transfer funds to each other. It handles 60 percent of American domestic transactions by value or about $360 billion a day.[2] The system was fully automated in 1973 with all of the Federal Reserve district offices having communication switches to which Federal Reserve Banks, branches, offices, the Department of the Treasury, and member banks are connected nationwide through a central switch facility in Culpepper, Virginia. This system allows for same-day movements of funds among member banks and helps banks in the efficient handling of reserve balances.

BankWire/CashWire is a private communications system serving about 185 banks in 75 cities throughout the United States and Canada.[3] BankWire transmits an average of 18,000 messages per day with a daily value of transferred funds exceeding $120 billion. In addition to funds transfers, the system is used for a variety of interbank business communications including loans and account balances. CashWire recently began operations in 1982 as a new service introduced by the BankWire organization. While BankWire essentially acts as a communications facility over which one bank advises another to transfer funds, CashWire is a true payment system, functioning as the settling agent on behalf of participating banks.

CHIPS was established in 1970 and operates out of New York City. It processes 90 percent of all international dollar transfers made.[4] Over 90

---

[1]"Time for the Industry to Improve Efficiency of Wire Transfers". ABA Banking Journal. April, 1983, p. 58.

[2]"Electronic Banking Comes Out to Meet Its Customers". The Economist. October 2, 1982, p. 84.

[3]"Regulation of Electronic Funds Transfer: Impact and Legal Issues". Communication of the ACM. February, 1983, p. 112.

[4]"Electronic Banking Comes Out to Meet it Customers". The Economist. October 2, 1982, p. 84.

banks participate, 56 of which are New York branches of foreign banks. In 1981, CHIPS processed an average of 70,000 transactions worth about $120 billion every day.

SWIFT was set up in Brussels in 1973 and began operation in 1977. SWIFT was developed as the need arose in the international banking community for a faster and more reliable payment message handling system. There are over 900 members in 39 countries, of which 150 are U.S. banks.[1] SWIFT handles an average of 250,000 international transactions a day in many different currencies. SWIFT has been a leader in providing standard formats for international payments.

Most of the largest banks also have their own telecommunications networks joining their own foreign offices and branches. One example is Citibank which maintains a private leased line telecommunications network with a main switching center in New York, and other switching centers in London, Hong Kong, and Manama (Bahrain). Some 80 banks in 65 countries are interconnected.

Groups of affiliated bankers may also have regional networks. One example is the Western Bancorp network that links 22 banks in 11 states in the western United States.

In 1982, the Bank Administration Institute (BAI) conducted a survey on the operations and automation status in funds transfer.[2] The information was collected from 127 commercial banks, with 70 percent of them being regional center banks. The respondents rated the four major funds transfer networks according to the service criteria presented in Table 3-1. The criteria used are listed in sequence of most important to least important. Overall, SWIFT received the highest rating by the respondents, BankWire and FedWire tied for second place and CHIPS had the lowest rating.

Operation and Automation Status

The automated integration of fund transfer systems by commercial banks is on the rise. In 1982, 23 percent had integrated wire systems with 44 percent planning to change over during the next three years. Table 3-2 shows the extent of automated/integrated systems in 1982 and those planned in the following three years.

---

[1]"SWIFT". ABA Bankers News Weekly. February 28, 1984, p. 8.

[2]Bank Administration Institute. Studies in Funds Transfer. Rolling Meadows, Illinois, 1982.

Table 3-1

QUALITY RATING OF MAJOR ELECTRONIC FUNDS TRANSFER SYSTEMS[1]

Service Factor	Factor Importance Rating	Funds Transfer Systems Rating			
		FedWire	BankWire	CHIPS	SWIFT
System Availability (free from down-time)	1.1	2.3	2.1	1.5	1.5
System Capacity/Speed	1.4	1.9	2.2	2.8	1.5
Settlement Convenience and Risk	1.6	1.7	2.1	1.9	1.5
Clear Message Format	1.7	2.2	2.2	2.9	1.3
Balancing Capability	1.9	1.9	2.8	2.3	1.6
Response to Questions About Day-to-Day Operations	2.1	2.3	2.3	2.5	2.0
Responsiveness to Industry Needs	2.1	2.7	2.3	3.0	1.7
Ability to Support Automated Reconciliation	2.3	1.9	2.4	3.0	1.9
Cost	2.4	2.5	2.5	2.9	1.9
History Retrieval Capability	2.5	3.0	2.2	3.7	1.9
Handling of Non-Funds Messages	2.8	2.7	2.1	3.8	1.6

[1]The quality rating scale used was: highest quality = 1, lowest quality = 5.

Source: Bank Administration Institute. Studies in Funds Transfer. Rolling Meadows, Illinois, 1982.

Table 3-2

PROPORTION OF COMMERCIAL BANKS WITH AUTOMATED/INTEGRATED FUNDS TRANSFER SYSTEM -- 1982

System	Integrated With[3]					
	FedWire	BankWire	CHIPS	SWIFT	TWX/Telex	Own[1]
FedWire		19%	3%	3%	6%	11%
Future[2]		29	13	26	28	22
BankWire	19%		2	2	8	11
Future[2]	29%		11	23	26	19
CHIPS	3	2		3	1	2
Future[2]	13	11		18	13	9
SWIFT	3	2	3		1	3
Future[2]	26	23	18		26	17
TWX/Telex	6	8	1	1		5
Future[2]	28	26	13	26		21
Own Private System	11	11	2	3	5	
Future[2]	22	19	9	17	21	

[1]Private System

[2]Future -- refers to future plans within a 3-year horizon.

[3]Elements in the diagonal are left blank denoting the requirement of at least two systems for integration purposes.

Source: Bank Administration Institute. Studies in Funds Transfer. Rolling Meadows, Illinois, 1982, p. 37.

Table 3-3 shows the increasing percentage from manual to automated systems in three years of the banks without integrated systems.

Table 3-3

FUNDS TRANSFER SYSTEMS CURRENT AUTOMATION STATUS AND FUTURE PLANS -- 1982

	FedWire	BankWire	CHIPS	SWIFT	TWX/Telex	Own
Current Automated Plan	41%	20%	50%	49%	25%	46%
Future Automation Plan (3-year horizon)	86	72	67	82	70	75

Source: Bank Administration Institute. Studies in Funds Transfer. Rolling Meadows, Illinois, 1982, p. 37.

The use of software packages versus in-house developed software is presented in Table 3-4. Increasingly, banks are making more use of package software than custom developed software for their automated systems.

Table 3-4

SOFTWARE USE IN AUTOMATED FUND TRANSFER SYSTEMS

	Custom In-House Software	Custom Software Developed by Contractor	Software Package With Substantial Modification	Software Package With None or Minor Modification
Actual Method	33%	22%	22%	23%
Method if Done Over	25	13	22	40
Method in Progress	24	14	21	41

Source: Bank Administration Institute. Studies in Funds Transfer. Rolling Meadows, Illinois, 1982, p. 39.

Thirty-two percent of the banks combined their foreign and domestic transfers in 1982 with 44 percent planning to in the future.

Table 3-5 shows the present and future projections of funds transfer through third party services (e.g., National Data Corporation or Interactive Data Corporation) or bank supplied connections to cash management/balance reporting systems.

Table 3-5

PROJECTIONS OF FUND TRANSFERS THROUGH THIRD PARTY SERVICES

	Percent of Commercial Banks Using	
Year	Third Party Services	Bank Supplied Connections
1982	1.5%	2.7%
1983	2.1	4.5
1984	3.0	5.3
1985	3.2	6.6

Source: Bank Administration Institute. Studies in Funds Transfer. Rolling Meadows, Illinois, 1982, p. 32.

Cash management services, either supplied by banks or third parties, are designed to assist the corporate user in the better utilization of their funds. Cash management include speeding up receivables; collecting, transferring, and concentrating cash; monitoring balances; and controlling and making corporate disbursements. The objective is to know the location of the funds so as to be able to move them into an earning capacity as soon as possible. Corporations consider wire transfers a major tool, not only for mobilization of cash, and elimination of float in intracompany payments, but also for disbursing large-dollar intercompany payments. Table 3-6 presents some typical examples of wire transfer usage.

Problems and Barriers to Growth

A survey of use of EFT by commercial banks conducted by the BAI, summarized in Figure 3-1, revealed that the most important concerns of management are message security and lack of uniform standards throughout the industry. The two concerns are interrelated since a lack of uniform standards force the banks to relax controls in order to meet the competitive pressures of customer service.

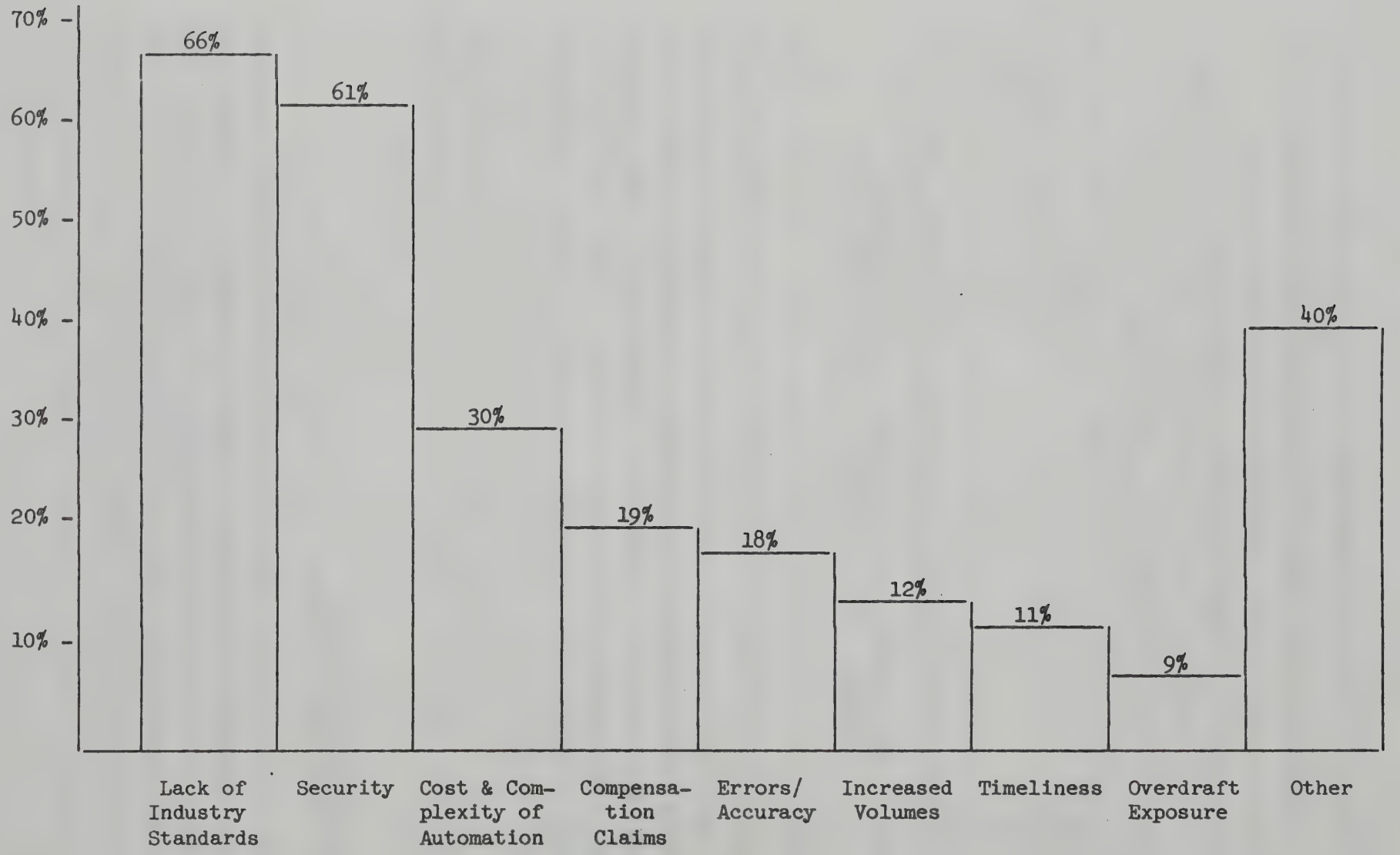


Figure 3-1: KEY MANAGEMENT CONCERNS IN REGARD TO ELECTRONIC FUND TRANSFERS

Source: Bank Administration Institute. Studies in Funds Transfer. Rolling Meadows, Illinois, 1982, p. 16.

Table 3-6

WIRE TRANSFER USAGE BY TYPE OF CORPORATION

Used For	Reason	Most Frequent User
Money Mobilization	to improve fund utilization	conglomerates, large national and international, geographically dispersed
Intracompany Payments	to ensure that funds arrive on the date needed, and to eliminate float	diversified corporations
Intercompany Payments	to earn a special cash discount, extend the payment date, and conform to sales terms and industry practice	utilities, large national manufacturing, financial and corporations dealing in the money market
International Payments	to speed fund movement	large international

Source: "Electronic Funds Transfer". Coopers and Lybrand Newsletter. 1979, p. 6.

The BAI survey found that encryption techniques were used by 11 percent of the banks, with the majority of encryption being used over the SWIFT network. Much of the security concerns uncovered in the survey refer to manual procedures and policies rather than complex technical issues, such as data encryption. Thus, rapid improvements of controls could occur if uniform standards and procedures were agreed upon by the banking industry. The survey found that 46 percent of the funds transfer agreements do not limit transfer amount; 48 percent do not specify time deadlines; liability for compensation is specifically covered in 41 percent of the agreements; only ten percent would refuse to accept a funds transfer not covered by an agreement from an existing customer and only 24 percent would refuse the transfer request from a new customer.[1]

Efforts for funds transfer agreements are hampered by the lack of applicable laws, definition of common banking practice and forum to voice procedural concerns.

[1]Bank Administration Institute. Studies in Funds Transfer. Rolling Meadows, Illinois, 1982, p. 16.

Transfers involving only one of the four networks seldom cause banks much problem. The problems arise when they must handle transfers that involve more than one network or when a transfer requires additional information that cannot be accommodated by a network's format. These situations can lead to inefficient and costly operating procedures for banks, including exception processing, frequent delays, exposure to loss, customer dissatisfaction and compensation claims.

The banks in the BAI survey reported a dramatic 360 percent increase in compensation claims for damages resulting from network malfunctions. Sixty-three claims were reported during the three years before 1981 and 114 were reported from 1981 to June, 1982.

Banks have been developing automated systems to bridge the incompatibility of the wire networks. The ABA has published a set of guidelines for network format conventions and conversion rules in order to help banks automate their funds transfer process.

Some within the industry have questioned the appropriateness of keeping four discrete networks.[1] Originally each of the networks were created to serve a specific purpose and select constituency. Over time, however, a significant number of banks became active users of all four systems. The result has been a fragmented, inefficient system. A study by Arthur D. Little[2] of the payment system observed that activities proceed component by component. The resulting competition among the various payment networks does not insure or encourage coordination and may lead to inefficient use of resources. Suggestions to unify the wire transfers include combining BankWire and CHIPS, and setting up a nationwide settlement feature within SWIFT. The Steering Committee of the SWIFT U.S. National Group has requested that the Association of Reserve City Bankers look further into the subject.

---

[1]Quoted in Donald R. Hollis. "Time For the Industry to Improve Efficiency Transfers". ABA Banking Journal. April 1983, p. 58.

[2]Ibid.

4

RETAIL ELECTRONIC FUNDS TRANSFER

BACKGROUND

In the 1960's the American Bankers Association (ABA) and the Federal Reserve Board advocated a payment system based on electronics and telecommunications instead of the conventional paper-based payment system. It was believed that a network of electronic funds transfer (EFT) systems would make economic sense and help control a payment system that costs approximately one percent of the Gross National Product.[1] Roughly two-thirds of this cost is associated with the check as a means of payment. An EFT system would provide an inflation hedged, machine-intensive payment system that would replace the labor-intensive and relatively unprotected from inflation, paper-based payment system.

As of today, the paper-based system is still the prevalent system. There are indications, however, that the United States is entering the beginning phase of an EFT system that reaches to the individual -- retail EFT. The first step that can be seen today is the expanding use of automated teller machines (ATM). Following right behind ATMs will be point-of-sale (POS) service in retail stores. Developing on a different but concurrent path will be the advent of home banking via videotex systems.

---

[1]Arthur D. Little, Inc. The Consequences of Electronic Funds Transfer. Cambridge, Massachusetts. June 1975, p. 8.

The change to an EFT payment system will take place in an evolutionary path throughout this and the coming decade. The paper-based system will continue to be with us for quite a long time as the number of checks will not start to diminish until at least 1990.[1] There will be large capital expense necessary for the conversion to an EFT payment system. A study conducted by IBM in 1978, forecasted 1985 EFT equipment needs to be 32,000 ATM's and 50 automated clearing-houses to handle just 15 percent of check-type payments through direct deposits, and 40,000 POS terminals to replace another six percent of the check volume. The cost of this would be $2.7 billion.[2]

Current Payment Methods

The personal checking account is the backbone of our payment system. In between the use of currency for small purchases, and the use of sophisticated wire transfers for high-value transactions, the personal checking account is the device most Americans pay for. More than four out of five American households have checking accounts. A typical household writes 20 checks a month which accounts for 50 percent of the checks in the economy[3] (see Table 4-1).

People write checks for three general reasons according to a 1979 study by the Bank Administration Institute (BAI): to acquire cash, to make purchases over the counter, and to pay bills (see Table 4-2). If checks are to be displaced then there must be a better alternative to accomplish one of these functions.

Table 4-2

DISTRIBUTION OF PAYMENTS
(1979)

Retail Purchases	32%	Bill Payment	50%
Cash Acquisition	8%	Other Individuals	9%

Source: "Displacing the Check". Federal Reserve Bank of Atlanta Economic Review. August 1983, p. 8

[1]"Displacing the Check". Federal Reserve Bank of Atlanta Economic Review. August 1983, p. 44.

[2]Ahmed S. Zaki. "Regulation of Electronic Funds Transfer: Impact and Legal Issues". Communications of the ACM. February, 1983, p. 116.

[3]Arthur D. Little, Inc. The Consequences of Electronic Funds Transfer. Cambridge, Massachusettts, 1975, p. 89.

Table 4-1

DISTRIBUTION OF CHECK VOLUMES IN THE U.S.
BY WRITER/RECEIVER CATEGORY -- 1974

Check Writer Category	Check Receiver Category	Percent of Total Checks
Government	Individual	5.0
	Business and Government	2.0
	Subtotal	7.0
Business	Individual	25.5
	Business and Government	17.5
	Subtotal	43.0
Individual	Government	1.5
	Individual	3.5
	Business	
	-- retail	20.0
	-- cash	6.0
	-- banks	3.5
	-- national credit cards	2.5
	-- insurance	3.0
	-- utilities	4.5
	-- professional	2.5
	-- hotels	0.5
	-- contributions	1.5
	-- other	1.0
	Subtotal	50.0
TOTAL		100.0

Source: Arthur D. Little. The Consequences of Electronic Funds Transfers. Cambridge, Massachusetts, 1975, p. 89.

Problems With Existing Payment Methods

The difference perceived by consumers between checks and the other EFT alternatives should increasingly favor the EFT alternatives as the cost of checking becomes more expensive. Financial institutions are increasing their checking fees because of higher costs to them. What once were non-interest-bearing checking accounts have now moved to interest-bearing NOW accounts. The introduction of Super NOW accounts has moved deposits to accounts that came close to paying market interest rates. In 1979, banks were paying the highest rates on one-half of their accounts. After raising their rates to compete with money market funds, banks are now paying the highest rates on two-thirds of their deposits.[1] At the same time, the cost of check processing continues to rise along with the cost of labor, transportation, Federal Reserve processing, and other costs.

With bank costs rising for check processing, banks are beginning to charge substantial fees for writing checks. Basic banking services for a household have increased from $90 in 1979 to over $180 a year in 1983, and now make up 24.8 percent of a bank's income as opposed to 19.2 percent in 1979.[2] Consumers are just beginning to be aware of the true cost of checking, as financial institutions have gradually increased their fees over time. Merchants are also growing disenchanted with personal checks. Many supermarkets levy a fee for cashing checks or restricting the amount of cash for which a check can be written, even with a purchase. Some make it very inconvenient by having time-consuming approval methods, and a few merchants refuse to accept checks.

An example of the costs to a merchant for checks can be found in the retail grocery industry where a typical supermarket in 1981 cashed 2,786 checks per week -- a 63 percent increase from 1976. At a cost of about 45 cents per check, an average store paid about $1,250 a week for check cashing. Since the average store has weekly sales of $150,000, checking costs now amount to 0.83 percent of sales compared to 0.46 percent in 1976. This is nearly equal to a supermarket's net margin which has been about one percent in recent years.[3]

---

[1] "Complaints Rise Over Fees for Bank Services". Washington Post. April 12, 1984, p. A-1.

[2] Ibid.

[3] "The Debit Card at The Crossroads". Federal Reserve Bank of Atlanta Economic Review. March, 1983, p. 42.

For consumers, the current alternatives to the check are cash and credit cards. Table 4-3 shows retail customer's payment habits as indicated in a nationwide survey conducted by Payment Systems, Inc. during November and December of 1981.

Table 4-3

TYPICAL HOUSEHOLD PAYMENT METHODS -- 1981[1]

Type of Retailer	Cash	Check	Bank Credit Card	Credit Card	Do Not Purchase
Food Supermarkets	65.3%	47.8%			
Major Department Stores	50.9	33.8	13.2%	26.8%	
Furniture/Appliance Stores	32.1	36.5	14.1		18.1%
Discount Department Stores	62.0	28.4	9.4		10.7
Men's or Women's Clothing Stores	51.9	35.6	15.0		7.7
Gasoline Service Stations	64.4	8.9	4.0	25.5	7.6
Restaurants (out of town)	72.2	3.1	16.7		9.0
Restaurants (at home)	85.4	7.3	8.5		5.1
Airline Tickets	32.2	20.3	16.3	6.1	30.4
Hotels/Motels	46.2	12.8	23.8		18.5

[1]Figures in blank denote no use of this payment method. Figures do not add because of rounding.

Source: "The Debit Card At The Crossroads". Federal Reserve Bank of Atlanta Economic Review. March 1983, p. 36.

Issuers of bank credit cards, proprietary department stores and gasoline station credit cards, are also experiencing similar cost pressures in check processing. Card issuers have recently employed several strategies to improve credit card profitability. Some banks have introduced a fixed annual service charge. Others introduced a transaction fee every time the card was used. Other banks have increased the interest rate charged or reduced the grace period before interest charges begin to accumulate. Many merchants have lowered the

limits before authorizations are required. Others use separate checkout counters for credit card users. Some oil companies, such as Atlantic Richfield, have solved their credit card costs by eliminating their card altogether. Others offer discounts for cash purchases. Thus, credit card customers are experiencing increased costs and inconvenience when making payments, just as check users.

Security and fraud is also increasing for credit cards. Fraud and credit losses in the VISA U.S.A. system increased from $94 million (0.63% of sales volume) in 1977 to $450 million (1.36% of sales volume) in 1980. VISA estimated that the total industry credit and fraud losses for 1981 were one billion dollars.[1]

Merchants and financial institutions bear significant expenses, such as armored car services, and secured storage of cash and theft insurance to handle cash transactions. Cash handling also adds more to accounting costs than credit card paper. In addition, there are more financial risks in allowing employees to handle cash, and mistakes and dishonesty are more prevalent.

The cost of handling cash at service stations is about four percent of sales compared to three percent for bank cards. Cash sales also invite robberies. Service station robberies increased 5.4 percent in 1981, the third increase in four years, although there has been a 15 percent decrease in the number of stations. In 1981, one out of eight stations were held up with an average loss of $372 for a total loss of $8.5 million.[2]

On top of the merchant problems, cash is dangerous to carry for consumers. It does not offer proof of payment and it has less of an ability for recourse action in disputed transactions.

RETAIL EFT TECHNOLOGY

The last few years have witnessed the emergence and adoption of technological solutions to the payments problem. These technological changes involve the beginning deployment of ATMs and the demonstrations of POS systems, the next step in the ladder of solutions to the retail payment system.

---

[1] Ibid., p. 41.

[2] "Displacing the Check". Federal Reserve Bank of Atlanta Economic Review. August, 1983, p. 21.

Automated Teller Machine

ATMs offer an alternative to the check for acquiring cash. By using a plastic card in an ATM machine, funds from a bank account can be converted directly to cash, whereas in the past, a check would have had to be cashed over the counter. Research has shown that it takes two ATM transactions to replace one check.[1] ATMs can also displace checks that are written for retail purchases as they are being installed in high traffic retail outlets such as supermarkets, convenience stores and shopping malls.

ATMs are the most popular EFT service and account for 70 percent of all EFT transactions. Over 9,000 banks have installed ATMs. In 1983, ATMs accounted for 3.75 billion financial transactions totalling $105 billion in ATM withdrawals and $214 billion in ATM deposits.[2] An IBM study on bank automation found that by 1986, off-line teller transactions will cost 82 cents, on-line teller transactions will cost 48 cents, and ATM transactions will cost 28 cents.[3] Table 4-4 shows the rapid increase in the number of ATMs over the last couple of years with a projection of over 100,000 machines by 1990.

Table 4-4

AUTOMATED TELLER MACHINES IN OPERATION -- 1980-1990

1980	1982	1983	1990
10,000	32,000	47,000	125,000

Source: Robert M. Garsson "Easy Money". Datamation. January, 1984, p. 33.

ATMs are also being used more frequently. The number of transactions per ATM per week increased 30 percent from 1980 to 1981, according to a BAI survey summarized in Table 4-5. The survey also found that 91.6 percent of all ATMs are located on bank property with the rate declining as ATMs move to retail locations. Banks are also strongly committed to on-line ATM operations as 92.8 percent of the banks surveyed operated on-line systems.

---

[1] Ibid., p. 8.

[2] Linda Fenner Zimmer. "ATMs 1983". Bank Administration. May 1984, p. 25.

[3] Quoted in Ahmed S. Zaki. Op. Cit.

Table 4-5

AVERAGE NUMBER TRANSACTIONS PER ATM PER WEEK

1978	1979	1980	1981
981	1,074	1,262	1,646

Source: Bank Administration Institute. 1981 Survey of the Electronic Funds Transfer Transaction System. Rolling Meadows, Illinois, 1982, p. 19.

Shared ATMs

Similar to the growth and popularity of ATMs, have been the proliferation of ATM networks. Forty percent of the ATMs are linked to one of the 150 regional or seven national shared EFT networks.

Industry-wide standards are needed for EFT and are just beginning to be tackled by the ATM networks. The first meeting of the EFT Network Council, a committee to develop standards, was held on June 5, 1984 in Washington, D.C. At an ANSI X9A meeting on April 19, 1984, David O'Connor, Chairman of the newly formed standards committee, claimed that at a meeting of seven national and regional ATM networks, the participants had no idea of ANSI standards. The first meeting on June 5th determined how the committee will relate to ANSI, ABA and International Standards Organization (ISO) efforts to help solve the immediate problem of network interface. Interfacing to a national network can be a technical burden that may require months to do at a cost of $10,000 - $30,000.

About one-half of the nation's networks have the capacity to support POS payments as well as ATM transactions. Those that do not, will have to replace their switch if they want to process POS payments. Roger J. Abouchar, Division Vice President of Anacomp, predicts that 500 additional switches will be installed by 1990 at a cost of $300,000 to $500,000 each.[1] Table 4-6 shows some characteristics of the nationwide EFT retail networks. Probably the most important aspect of the shared networks is the number of shared debit cards. Bank Network News estimates that there are now over 50 million shared ATM access

[1]Robert M.Garsson. "Easy Money". Datamation. January 1984, p. 34.

Table 4-6: NATIONAL EFT RETAIL NETWORKS

Network	Terminals	Card Base	Cost	Membership Composition
CIRRUS Oak Brook, IL	3,500 in 34 states	11 million	initiation fee plus $.75 per withdrawal and $.50 per inquiry; network keeps $.25.	12 owners and 600 sponsored members
EXPRESS CASH New York, NY	1,011 in 16 states	2 million	no initiation fee; transaction fee $1; network keeps $.50.	900 financial institutions
THE EXCHANGE Clifton, NY	2,500 in 35 states	3 million	not available	583 mostly smaller financial institutions.
PLUS SYSTEM Denver, CO	2,200 in 47 states	19 million	proprietary members pay a $200,000 initial fee, $.75 transaction fee; network keeps $.25; sponsored members pay $500 initial fee.	34 proprietary members and 1,100 sponsored members; 10% are savings associations
MASTER TELLER New York, NY	1,500 in 24 states	not available	no initiation fee; $1.64 transaction fee transmitted to ATM owner.	160 financial institutions
NATIONET Brown Deer, WI	5,000 in 26 states	expected 20 million	$5,000 stock purchase plus $25,000 initiation fee; transaction fee $.70; network keeps $.15.	13 network members
VISA San Francisco, CA	50 now, 6,000 committed worldwide; 3,800 committed in U.S.	expected 30 million	not available	230 banks

Source: "ATM Networks Span the Nation". Savings and Loan News. April 1983, p. 51 and "National Networks Postpone a Shakeout". Bank Network News. December 16, 1983, p. 2.

cards, up from 29 million last year. The shared debit card base will help bring about the next and larger phase of retail EFT -- direct debits at the POS. Every national network and many regional networks are initiating POS projects or looking at it for the future.

Nonbank Locations

To gauge the extent of ATM activity in retail establishments, the Federal Reserve Bank of Atlanta did a survey in August, 1983 of 35 of the largest grocery and convenience store chains in eight southeasten states.[1] Grocery and convenience stores were selected as a testing ground for EFT activity because:

- grocery establishments cash 70 percent of all checks written at the retail level;
- convenience stores want to eliminate cash thereby discouraging robberies;
- both provide a large number of widely dispersed stores open for long hours;
- customer traffic is regular and heavy;
- most payments are drawn against local financial institutions; and
- both may pave the way for EFT in other stores such as gas stations and department stores.

The survey results summarized in Table 4-7, found that 23 of the 35 chains questioned either have ATMs installed or plan to install them in the next two years. Two others are conducting ATM tests in other parts of the country. The stores that had no plans for ATMs frequently cited as their reason that their businesses were rural or small town in nature, and that bank site ATMs hardly exist, and the transaction volume would not justify installing in-store ATMs.

Two distinct patterns of installation appear. The first are the stores in which a single bank installs ATMs (generally one to ten) and only that particular bank's customers can access the machine. The other pattern is one where ATMs (ranging from 50-100 machines) will be installed as part of a large regional network comprised of many banks. The latter pattern is increasingly predominant as more banks are joining networks and the large cardholder base makes massive implementation of ATM regional networks economically feasible.

---

[1]"In-Stores ATMs: Stepping Stone to POS". Federal Reserve Bank of Atlanta Economic Review. January, 1984, pp. 31-42.

Table 4-7

SURVEY OF ATM ACTIVITIES IN 35 SOUTHEAST STORE CHAINS -- 1983

Supermarkets	Amount	Convenience Stores	Amount
ATMs Installed	8	ATMs Installed	3
Within Six Months	3	Within Six Months	3
Definite Plans to Install	3	ATM Pilots Elsewhere	2
Within Next Two Years	3		
No Plans	10		

Source: "In-Store ATMS: Stepping Stone to POS". Federal Bank of Atlanta Economic Review. Jaunuary 1984, p. 34.

As shown in Table 4-8, the largest motive for having ATMs in stores was found to be for customer convenience. Another motive, mainly for convenience stores, was their desire to increase customer traffic in stores in the hope that customers, after entering the store to obtain cash, will purchase a few items. Reducing check volumes and cost was also a major concern. While convenience stores do not cash many checks, grocery stores do, and many complained about the extent to which they act as surrogate banks. Twelve claimed to cash more checks than the local banks. Not only do they have to pay for the labor and processing costs involved, they also have to pay a fee for each check deposited. ATMs represent a role reversal. Instead of paying processing costs and bank deposit fees, the stores receive a rental fee for the space in which the ATM is located. The owner of the ATM and the operator of the switch split the transaction fee. The bank of the customer whose account was debited pays the transaction fee, or, may in turn, pass the charge on to the customer. But the retailer does not pay anyone. The store may even generate income if it also owns the ATMs.

One example of a store installing its own ATMs is the Publix Supermarket stores in Florida. Publix has installed 125 ATMs in their stores thus far and has announced that they may install up to 3,000 ATM/POS terminals in their 260 supermarkets. Publix owns the terminals and the switch, and will charge financial institutions for the transactions.

Table 4-8

MOTIVES UNDERLYING ATM INSTALLATION IN SURVEY OF 35 SOUTHEASTERN STORE CHAINS -- 1983

	Supermarkets	Convenience Stores	Total
Increase Customer Convenience	13	7	20
Increase Customer Traffic	1	6	7
Reduce Check Processing Costs	11	1	12
Reduce Check Volume	8	1	9
Reduce Bad Checks	7	-	7
Reduce Cash Security Problems	2	-	2
Reduce Labor Involved	1	-	1

Source: "In-Store ATMS: Stepping Stone to POS". Federal Bank of Atlanta Economic Review. Jaunuary 1984, p. 34.

Financial institutions in Florida reacted rapidly to Publix's announcement. While previously committed to proprietary networks, 120 financial institutions hurriedly formed their own shared network in Florida as they feared a retailer-controlled POS system. Publix entry thus proved a stalemate breaker between proprietary versus shared networks and showed that if financial institutions will not provide an environment for POS activity, then merchants or other institutions can and will.

Another large announcement of nonbank ATMs and a demonstration of the appeal of a universal debit card to retailers comes from First Texas Savings Bank who will install ATMs in all of the 1,000 7-Eleven convenience stores located in Texas. Before the offer was attractive enough for 7-Eleven, First Texas Savings had to win a Justice Department antitrust decision that enabled it to join both of Texas' major shared networks and thus provide a shared card base of 7.4 million. The convenience store will collect rent plus a transaction fee from the ATMs. The bank will collect fees from the other banks connected to the network.

Thus far, we have chronicled the rapid increase and popularity of ATMs, the growth in shared networks and the move of ATMs from bank locations into retail stores. These events now set the stage for the next step of the retail EFT payment system.

Point-of-Sale

Out of the 25 stores with ATM plans in the Federal Reserve Bank of Atlanta Study, 17 view the installation of in-store ATMs as a stepping stone to POS systems. Some even implied that ATMs were being installed solely as an intermediate step. While most retailers concede that POS is inevitable, only three have any firm plans regarding POS and seven claimed to have vague plans.

In addition to ATM and POS activity at grocery and convenience stores, there is much activity at gasoline stations. Twenty-three POS pilots are underway in the petroleum industry. Oil companies are initiating POS payment systems at their gas stations to reduce processing costs, float, and robberies, and for their general movement to unmanned, automated gasoline stations. Based on a ten percent interest rate, the total loss in float for the petroleum industry by credit card purchases was $411 million in 1982.[1] In addition, credit card purchases also produce losses in fraud and unauthorized purchases. Arco has four pilots underway. Chevron has thousands of NCR cash registers that can be upgraded to POS. Gulf intends to install 3,000 POS devices by 1985. Phillips intends to have 4,000 stations automated by 1985.[2]

Exxon USA began tests in Phoenix where it will issue its own debit card to customers which will debit their accounts through the Automated Clearinghouse (ACH) system. When customers purchase gasoline, Exxon will initiate an ACH debit through Chase Manhattan Bank. Customers will receive the same five cents a gallon discount that Exxon gives its cash customers. For Exxon, the advantage is that it can issue a debit card to any one with a checking account without having to wait for the banking industry to come to terms with POS.

Mobile Oil is introducing its own computerized POS network. Since November 1983, Mobil customers can use their bank ATM cards to pay for purchases at 70 gasoline stations in the Washington, D.C. region. By the end of 1984, Mobil hopes to have 2,400 outlets across the country linked by computer to the company's headquarters and participating banks. When fully operational, the electronic system will handle traditional credit card transactions as well as bank debit card transactions.[3]

---

[1]Edith Myers. "Is Real POS Coming". Datamation. December 1983, p. 99.
[2]Ibid.
[3]"The Race Is On". The Banker. March 1984, p. 86.

The U.S. Department of Agriculture (USDA) is conducting an 18 month experimental POS program in the supermarkets of Reading, Pennsylvania. The program will replace paper food stamp coupons with an electronic POS system in hopes of reducing the illegal trafficking, mail fraud, and lost and stolen coupons. Food stamp households will receive magnetic cards with biographic information and be assigned a personal identification number (PIN). The system can handle commercial debit and credit cards as well as food stamps so the retailers can have the option of offering an electronic payment system to all of their customers. The program will credit daily the value of the food stamps to the merchant's account. Food stamp funds will be distributed by the Federal Reserve Bank to a local bank which will transmit the funds to the merchant's bank.

Factors Influencing POS Growth

The factors which will affect POS in the future include:

- installation of computer equipment at the store level by retailers;
- advances in POS technology;
- increased pressure to move away from paper-based transactions by merchants and financial institutions;
- expansion of the critical mass of cardholders; and
- consumer acceptance.

Merchants, especially food stores and department stores have been installing electronic cash registers (ECR), computer systems, and telecommunication lines for their stores to reduce labor expense, for inventory management, and for energy management. EFT can now be an add-on service to merchant's computerized systems. Five banks in California, who have joined forces to set up a shared POS network, indicated that their action was taken mainly due to the sophisticated transaction equipment that retailers are installing.

The upgrading of merchant's existing computer systems will not be problem free. Up until recently, it was thought that automated supermarkets could readily accept debit cards simply by attaching card readers and PIN keypads to their ECRs and use their in-store computers to send authorization requests to the bank's debit card networks. However, many ECR systems simply cannot be upgraded to handle card transactions and retrofitting newer ECRs is complex and expensive. For example, to upgrade NCR corporation's popular NCR 255

electronic checkout system would entail more than adding PIN pads and magnetic strip readers: the terminals must have special function keys and extra software, and extra memory must be added to the store's computer to handle the protocols required for communication with the debit card networks.[1]

The alternative to upgrading one's ECR would be to install a separate system alongside the current one or to buy a completely new system. Supermarkets that are retooling can now purchase systems that are fully capable of handling debit card transactions. However, the cost of an automated POS system for supermarkets is well over $100,000 per store. In contrast, a "stand-beside" system can be installed in supermarkets for $16,000 to $30,000. The stand-beside systems generally include PIN pads and card readers at each checkout counter, plus a special computer that drives the terminals and links them to debit card networks.

The dilemma facing supermarkets can be seen in Giant Food Inc. in Washington, D.C. Giant has first generation IBM systems in their stores which cannot be upgraded to handle debit card transactions. Giant estimates that installing new systems with transaction processing capabilities would cost $24 million for its 130 stores. The alternative of installing stand-beside systems would cost the chain $6-$7 million. As a result, Giant does not see any economic justification for changing its POS system solely to handle debit cards, since the company estimates that it will save only 1.3 cents for every check transaction that is replaced. Instead, Giant will add modern checkout systems when it is appropriate to meet its grocery needs.[2]

Alternatively, Bill Bishop, a Chicago-based consultant for supermarkets, believes that debit card processing systems will be a good investment for supermarkets, and he questions Giant's estimates believing that supermarkets should be able to save four cents on every transaction.[3]

Financial institutions and gasoline stations typically base their debit card on the magnetic-stripe technology that is used on credit cards. Grocery stores, on the other hand, base their technology on an optical scanner that reads the bar codes on products. Department stores typically prefer optical character recognition (OCR) to read information from merchandise tags and proprietary credit cards. To harness everyone's technology base, VISA has

---

[1]"Terminals: A Dilemma for Supermarkets". Payment Systems Newsletter. May 7, 1984, p. 1.

[2]Ibid. p. 5.

[3]Ibid.

developed an electronic debit card that includes a magnetic stripe, bar code, and OCR information. The card is being tested this year. Although it does not require a PIN now, in the future the card will require it. This will entail that merchants have PIN pads capable of encrypting PINs. VISA also has plans to use electronic signature verification as a means of positively identifying customers.

POS terminal systems have been getting cheaper, more reliable, and easier to service. The terminals of the past were teller terminals installed in merchant locations. They were expensive and difficult to use in a retail environment. Their cost dictated that only one or two could be used in a retail store.

Diebold has come out with a modular system that can drive up to 60 terminals and eight dedicated communications lines. It can be hooked up to ATMs, teller terminals, POS terminals, energy management systems, electronic security devices and automated fuel systems, and only cost $20,000. NCR has developed a modular ATM/POS terminal for the retail environment. It can handle four currency denominations, can handle deposits, and reads all three tracks on magnetic cards. It sells for $15,000 - $20,000 per machine. NCR is also marketing a product line of self-service terminals which will sell gasoline, airline, theatre, and ski lift tickets.

The cost of a POS transaction is already lower than the cost of a paper-based transaction. Currently, POS systems charge transaction fees of about 20 cents compared to 45 cents for the cost of a paper-based transaction.[1] The cost advantage is expected to increase over time. Electronic POS is not labor and transportation intensive, but relies on intensive use of computer and telecommunication systems which have been declining in cost.

As opposed to ATMs which started out as proprietary networks, POS will start out as shared networks. To make POS economically feasible, a critical mass (some say 75 percent of debit cardholders) will have to be able to access the retailers POS system. Shared ATM networks are bringing about this realization. There are now 50 million ATM shared network cards compared to 29 million in 1982. This represents 67 percent of all debit cards in the United States.

No matter how attractive EFT is for merchants and financial institutions and how much the technology progresses, POS will ultimately depend upon consumer acceptance. Presently, consumers perceive debit cards as just another way to do

---

[1]"In-Store ATMs: Stepping Stone to POS". Federal Reserve Bank of Atlanta Economic Review. January 1984, p. 41

something that checks, cash, and credit cards already do. Consumers may even perceive debit cards as being inferior to traditional payment methods as they lose float and control of stop payment orders. Only when consumers begin seeing an economic advantage will they begin to adopt debit cards. The perception of debit cards should become more appreciative as financial institutions and merchants begin pricing the payment methods at their true cost. In addition, consumers will start realizing the other benefits of debit cards such as time and place convenience, need to carry less cash, and quicker checkout times. According to a 1983 Food Marketing Institute survey, 39 percent of consumers place the greatest priority on quick checkout. Lower prices ranked second. A typical POS transaction takes 10-15 seconds. Cash takes 27 seconds and checks require even longer.[1]

Consumer acceptance of debit cards will also be helped by the large majority who already carry ATM cards and are familiar with using transaction terminals and PINs. Retail stores who install ATMs will also help condition the consumers to the transition to POS.

The Federal Bank of Atlanta sees the second step of electronic POS payments taking place between 1985 and 1989. They predict that by 1987, debit cards will account for 15 percent of all retail purchases out of checking accounts.[2]

BARRIERS TO ADOPTION AND USE OF TECHNOLOGIES

The next five years will witness the rapid growth of ATMs and the initial period of deployment of POS terminals. This growth period is anticipated in view of a convergence of economic and technological factors. The only clouds in the horizon concern the lack of compliance with communication protocols in the ATM networks and the security problems concerning EFT transactions.

Economic and Technical Aspects

The economics in the use of ATM machines by the banking sector and retailers has been discussed earlier. The costs to the banks per ATM transaction is 40 percent less than the cost per on-line letter transaction and 65 percent less

---

[1] Ibid. p. 41.

[2] "Displacing the Check". Federal Reserve Bank of Atlanta Economic Review. August 1983, p. 41

than the cost per off-line teller transactions.[1] The consumer is able to save the bank charges for checks processed and, in addition, to save time spent in transactions with tellers.

The same is true of the deployment of POS terminals with their cost and time savings for retailers, banks, and consumers.[2] Technological changes have brought down the cost of POS terminals which now are more reliable and easier to service. While the growth of shared ATM networks has contributed to gaining the critical mass of cardholders needed for the economic feasibility of POS systems, in the end this feasibility will depend on consumer acceptance. However, given the expected future increases in bank charges for processing checks, consumer acceptance may be realized faster than many realize. By the early 1990s there will be a huge mass of households experienced with ATM cards, making the transition to POS easier.

Standards and ATM Networks

At present the rapid growth of ATM networks is occurring without adherence or compliance with communications protocol standards. The current standards are, in fact, de-facto standards set by the larger networks. Industry-wide standards are needed for EFT and are just beginning to be tackled by the ATM networks. The first meeting of the EFT Network Council, a committee to develop standards, was held on June 5, 1984 in Washington, D.C. At an ANSI X9A meeting on April 19, 1984, David O'Connor, Chairman of the newly formed standards committee, claimed that at a meeting of representatives of seven national and regional ATM networks, the participants were not aware of ANSI standards. The first meeting on June 5th determined how the committee would relate to ANSI, ABA, and International Standards Organization (ISO) efforts to help solve the immediate problem of network interface. This is an area that needs industry attention to ensure that different ATM networks can connect. If permitted to grow without attention to communications protocol standards, a barrier to rapid growth of shared ATM networks and POS transactions will be created.

Security

The security of EFT transactions poses threats to its growth. The security problem, because of its complexity and importance, is discussed in more detail in Chapter 5.

---

[1]Ahmed S. Zaki. Op. Cit.

[2]"In-Store ATMs: Stepping Stone to POS". Federal Reserve Bank of Atlanta Economic Review. January 1984, p. 41

5

ENCRYPTION AND SECURITY SYSTEMS

BACKGROUND

The rising use and dollar amount of wholesale and retail electronic funds transfer (EFT) has led to a parallel increase in concern about the security of these systems. The level of security required for EFT is established by assessing the risks. Risk assessment is composed of five basic elements:[1]

- Risk Identification -- Development of an inventory of resources, the threats that could affect them, and the ensuing adverse affects.
- Risk Evaluation -- Measurement of the financial risk inherent in each exposure in terms of probable frequency and severity of loss.
- Strategic Alternatives -- Identification of the cost and availability of risk reduction alternatives and insurance.
- Trade-Off Analysis -- Comparison of the liability of exposure to the cost of risk reduction alternatives, insurance, and self-insurance.
- Implementation -- Installation and monitoring of the selected alternatives.

---

[1]American National Standard for Personal Identification Number (PIN) Management and Security X.9.8. American Bankers Association, Washington, D.C., January 14, 1982, p. 28.

The effectiveness of a security program lies in providing protection at a realistic, workable level and at a reasonable cost. Control measures that are too stringent will not be practiced.

No system will be successful unless a sufficient number of individuals and companies are convinced that it is safe, reliable and respects their privacy. Violations of security would cause more harm than just the actual monetary loss incurred, as it would result in the reduction of operational efficiency if users turn to alternative payment systems.

Security in electronic payment systems are comprised of two distinct aspects -- operational reliability and vulnerability to deliberate tampering. Operational reliability is concerned with safeguards against accidental disclosure of confidential data; with backup measures against system failure; and with safeguards against negligent or ignorant operator use. Vulnerability is concerned with protection against unauthorized and intentional alterations or disclosures to commit fraud.

Of the two aspects, operational reliability is more often threatened, as data is rendered useless by mistakes rather than by intent to dishonesty. However, recent developments have made the vulnerability to deliberate threat an increasing problem in payment systems. These developments stem from technological advances and expansion, and from a greater public awareness of such systems.

The first development is the growth in the number of networks. Wholesale EFT has been increasing in the number and usage of these payment systems. In addition, there has been an explosion of retail EFT networks including automated teller machines (ATM) and point-of-sale (POS) systems.

Security problems are particularly encountered as these networks are interfaced with each other. The standardization that is needed for the network's interconnection reduces security by removing the uniqueness of an individual's network protection mechanism. The possibility that a breach in security at one point in the system may compromise security at many financial institutions becomes real and important.

In recent years, the centralized location of equipment, transaction records and processing programs has increased the dangers of accidental destruction or criminal fraud. Paradoxically, the current distributed systems have provided greater flexibility at the expense of increased security risk.

Once a large scale EFT system is in operation, upgrading of security features will be prohibitive because of the standardization and cost in the system. Also, the reliability of the components may be impaired by enhancing the security features of hardware and software once the design has been completed. Thus, the system may not be able to take advantage of the latest technological advancements. Criminal elements, however, will not operate under such constraints. This makes system design and security precautions crucial at the beginning stage of an EFT system and not as an afterthought.

The growth in the number of terminals has also led to the increase in vulnerability. In the early days of automation, physical and logical access to data and transactions was limited to a small number of persons who were easily identified. Access has now become much easier as technical knowledge and equipment has become widespread. Banks have greatly increased the number of terminals used in their internal systems and linked to payment systems. A Bank Administration Institute (BAI) survey found that the average number of terminals a bank has, is 500. The First Interstate Banks have at least 8,000, Mellon Bank has 6,000 and even the smallest bank surveyed by BAI had 50.[1]

Even more important is the increasing intelligence, functional capabilities and accessibility that these terminals offer. The unauthorized use of terminals is potentially one of the greatest threats to the security of an on-line computer system. This is aggravated by the increasing use of card-activated terminals such as ATMs, POS terminals and home terminals. This kind of terminal brings the accessibility of the payment system from the controlled environment of a bank or computer installation to the vulnerable freedom of streets, shops or private homes.

The proliferation of card-activated terminals also results in a greater public awareness of payment systems and their technology. This awareness extends to the honest person as well as to criminal elements.

The growth of EFT networks together with the easier access to them leads to a greater motivation for law breakers to perpetuate fraud. Larger interconnected worldwide networks provide for economies of scale for the criminal to invest in the time, knowledge and equipment to commit a crime. Figures reveal that the average computer crime nets about $650,000 while bank robbers get away

---

[1]Steven Ross. "Who is the Data Security Officer"? Magazine of Bank Administration. 1982, p. 54.

with about $9,000.[1] By transferring the money overseas, the criminal can be gone before the auditors even know it happened.

There is also the risk from the intellectual challenge to break the system for its own sake rather than for material gain. This type of activity is witnessed in the hacker or electronic rummaging problem that recently was given extensive media coverage in the case of the "Milwaukee 414s" high school kids.[2] The publicity and almost glorification given to these computer abuses together with the lack of seriousness of these crimes given by the public and courts could lead to the hacker problem snowballing into almost a fad by computer zealots eager to beat the system.

SECURITY SYSTEM COMPONENTS

Security considerations for an EFT system encompasses three subsystems: terminals, communication links, and computers.

Terminal Vulnerability

Terminal vulnerability can come from remote-access computer terminals, ATM machines or POS teminals. The problem for terminals is the illegal access to them by unauthorized persons. Authenticity of an individual within a financial system can be verified by 1) a physical or personal characteristics (e.g, signature, fingerprint, voiceprint), 2) personal item being carried (e.g., badge, magnetic card), or 3) something known (e.g., password, PIN).

Remote-access terminals provide users with the means to access distant computer systems by telephone. Security precautions can include passwords, software systems and data encryption. However, less than two percent of the EFT users who are vulnerable to penetration do anything more than just password security.[3] A password is the most extensively used control because of its simplicity and cost of implementation. A password, however, does not provide

---

[1]Paul Gillen. "Danger of Electronic Theft Seen Escalating". Computerworld. November 21, 1983, p. 25.

[2]The label "Milwaukee 414s", refers to the Area Code (414) where the events occurred. This label was popularized by the media.

[3]Paul Gillen. Op. Cit. p. 25.

positive identification. Passwords can be stolen, placed in unsecure locations and guessed. Using trial and error, a patient computer hacker can often uncover a valid password and unlock a company's computer software system with little effort. The major problem with a password approach is that users pick very simple and easy to remember passwords that are not changed frequently. The majority of computer crimes since 1972 have involved password penetration.[1] One study showed that 15 common words comprise 80 percent of all user selected passwords.[2] In order for the password to be an effective control, it should be difficult to guess, easy to remember, changed frequently, and well protected.

One way to stop the hacker problem is to use a call-back system. With a call-back system, access is denied to any computer outright if the caller is not dialing from a previously authorized location. This system removes the caller's ability to play with the system and guess a correct password.

ATM and POS terminal access is limited by using a password or PIN in conjunction with a plastic card, usually magnetically striped, that contains electronically encoded data. Two types of fraud are associated with PINs and plastic cards: lost or stolen cards and counterfeit cards.

The most obvious is the lost or stolen card with the criminal also knowing the PIN. This has been made easy by the practice of customers not safeguarding their PINs. Surveys in Syracuse, New York and in Wisconsin showed more than 50 percent wrote their PIN number on their cards or kept it in their wallet.[3] Counterfeit cards represent a far more serious threat, especially with the establishment of nationwide EFT systems. Flooding the country with thousands of counterfeit cards would affect many financial institutions and result in disastrous financial and consumer confidence loss.

The difficult part for the criminal in card counterfeiting would be to know the correspondent PINs. Counterfeiting the cards is not especially difficult. A simple, inexpensive method is called "skimming" which produces cards of uneven quality. Another method, called "buffer recording", produces higher quality cards but is electronically complex and more expensive than is "skimming".

---

[1] Ibid.

[2] Bill Streeter. "People, More Than Technology, Are Still Key to EFT Security." ABA Banking Journal. July 1982, p. 34.

[3] "The Bottom Line on Checkless Banking." Technology Review. February 1980, p. 48.

As mentioned previously, other identifying methods such as fingerprints, voiceprints and signatures could also be used. While these methods are not currently used to any extent and they need to be evaluated further for their practicability and reliability, their use should start being seen in the late 1980's to provide user authenticity. For fingerprints, a person would place his index finger on an input spot on the terminal. Computer pattern recognition would then be used to verify the person. A variation would be to have fingerprints mounted in an indentification card that the terminal could read (e.g., smart card or laser memory card).

Voice recognition offers an attractive advantage in that no special terminal equipment would be needed, other than a telephone. A user would speak a predetermined phrase which would be compared to the voice pattern previously stored for the user. The problem with this method is that voice characteristics can be influenced by one's health or emotional stress.

Signature verification involves a person writing his signature on a pressure sensitive pad. A comparison would then be made of not only the image but also of the dynamics involved when writing the name.

Communication Links Vulnerability

Communication links refer to the methods by which an EFT transaction is sent from one point to another. Communication links are the weakest point in an EFT system because they can be relatively easy to tap into, the potential dollar loss is huge, and it is difficult to detect and locate a wiretap. The easiest communications to tap are microwave and satellite linkups with telephone lines next and optical fibers being the most difficult. Wiretapping may be used passively or actively. In passive wiretapping, the offender only listens to the transmission to obtain data on the overall volume of operations, financial statistics, general patterns of money movement, PINs, or to scan for particular transactions. In active wiretapping, the transaction is not only monitored, but also modified. This is used to falsify records, steal information, disrupt business activity by confusing records, or send additional information at the end or in between legitimate data. Active wiretapping allows a knowledgeable person to intercept the flow of data of funds between two points and divert large sums of money to a clandestine location.

For active wiretapping as well as transmission and operator errors, message authentication can provide the best safeguard. Message authentication prevents the undetected modification or deletion of data in transmission, processing or storage. Message authentication can be used with or without data encryption. For nonsensitive information such as money transfers, stock market and news information, data encryption may not be necessary. It is only important to verify that no one intercepted and altered the data. Also, international transactions may pass through a country that monitors data and which may not allow encrypted data to pass.

Message authentication also makes it possible to establish an audit trail back to the originator of a transaction. In addition, the use of message authentication can restrict the unauthorized duplication of messages. This capability is especially important in the automated banking environment of an ATM terminal where a criminal could repeatedly send signals that would instruct the ATM machine to issue cash.

COMPUTER VULNERABILIY

The computer is primarily vulnerable to the people who operate it (e.g., programmers, tellers, equipment maintenance personnel) that have knowledge or proximity to the system that enables them to evade safeguards and control points. Most crimes have been committed by low-level staff such as clerks who notice that their mistakes are not caught rather than by higher-level staff. Of 1,293 computer-related fraud cases identified in the last three years, only eight were perpetrated by programmers.[1]

Cryptography can be used to protect information stored on computers. One way is to encrypt the disk and tapes so as to counter physical theft. Another method is to use hardware and software that marks the records with checksums to specify the sensitivity of information.

To make the best use of security features, system designers must design-in security from the outset. One fundamental consideration is the inclusion of adequate audit trails so that violators, their violations, and their attempted violations can be tracked. Software audit techniques includes reviews of

---

[1]Jake Kirchner. "Encryption Endorsed as Way to End Hacking Plan". Computer World. November 21, 1983, p. 13.

program listings, review of a program's logic and test input/output and confirming the results with expected results.

One specific case of providing software security is through the use of Cobol Missing Branch Indicator (COMBI). This provides the opportunity for auditors to examine and map program codes to determine whether all modules of the program are being properly executed. COMBI helps prevent against Trojan-horse programs that contain illegally inserted and completely unrelated program code. The code might steal data and pass it on to the writer of the Trojan-horse program. Without COMBI or a similar technique, internal fraud or privacy invasion could go undetected for an extremely long period of time.

A survey of 43 banks revealed that IBM was the leading vendor in computer hardware, software, and telecommunications. All 43 banks had IBM mainframe computers, large systems adaptable to high-speed, multi-purpose use. Ninety percent of the banks used specialized software to manage their massive data bases, to control their telecommunications network and to restrict access to data and system facilities. For data base management systems, IBM's product, IMS, is used by two-thirds of the banks for data access and sharing. For telecommunication software, IBM's CICS is used by 46 percent of the banks, 19 percent have IBM's IMS DB/DC, and 21 percent use both software packages. For security or access control software, 55 percent of the banks used Cambridge Systems' ACF2 and 19 percent used IBM's RACF.[1]

BARRIERS TO THE ADOPTION AND USE OF SECURITY TECHNOLOGIES

The most important of the emerging banking security technologies concern data encryption. Encryption in the United States relies primarily upon the Data Encryption Standard (DES) algorithm, developed by the National Bureau of Standards. This section describes the data encryption standard and the barriers to its adoption.

Applicable Technical Standards

The ANSI Committee X9E8 on Financial Services has adopted an authentication method, based on the DES algorithm, entitled Financial Institution Message

---

[1]Steven Ross. "Who Is The Data Security Officer"? Magazine of Bank Administration. 1982, p. 56.

Authentication (FIMA) X9.9. The DES is based upon an algorithm submitted by IBM and is also a Federal Information Processing Standard. The authentication method adopted by the committee ensures the:[1]

- validation of the authority of the sender;
- verification that selected contents of the message have not been altered in transit;
- use by both large and small organizations; and
- implementation in both automated and manual systems.

The message authentication process provides security against active wiretapping and transmission/operator errors. The authentication process includes the computation, transmission, and validation of a Message Authentication Code (MAC). The DES, which requires a secret key, is used to generate the MAC. The MAC can either be used on the complete message or on a select part. The MAC is added to the message by the sender. The message is accepted as authentic by the receiver if the same algorithm and secret key produce identical MACs. The equipment to perform data authenticity can cost from $2,000 to $3,000 per unit and each terminal site would have to have such a unit.

In the case of passive wiretapping, protection lies in either making the data useless if monitored or in making the acquisition of it uneconomical in comparison to other methods. However, research conducted by SRI International's Computer Security Group indicates that generally, encryption is the only cost-effective way to counter certain threats to information and communication systems.[2]

Barriers to The Use of Encryption

Encryption must be used in the financial community in the transmission and storage of a person's PIN. Such environments include ATM and POS activities. Encryption is made more complex as networks link together. Encryption requires

---

[1]American National Standard for Financial Institution Message Authentication, American Bankers Association, Washington, D.C., April 13, 1982, p. 4.

[2]Quoted in: Charles Cresson Wood, "Future Applications of Cryptography". Journal of Telecommunication Networks. Summer 1982, p. 66.

security modules at the various switching points and also requires that an ATM be able to encrypt a person's PIN. Not all ATM's installed have this capability. A retrofit encryption package costs about $1,000 from the major ATM manufacturers.

United States vendors primarily offer encryption devices based on the National Bureau of Standards' DES. Foreign vendors offer a variety of proprietary algorithms. The cryptographic strength of the foreign algorithms is usually significantly less than the DES. The fact that foreign algorithms are often weak is partially offset by the fact that foreign vendors rely on both the secrecy of their algorithms as well as the keys. In the case of the American vendors, since the DES algorithm is known and freely available, the security provided by the algorithm is based upon the protection of the cryptographic key from disclosure to unauthorized persons.

More than 35 major domestic and foreign vendors offer numerous encryption products built for different applications, techniques and equipment arrangements. These vendors have been struggling to survive, and others have taken their products off the market, however, because of a lack of interest.

The road blocks to the use of encryption are two-fold: level of perceived threat and economics. Banks have not been using encryption because there have been very few cases of known wiretapping. SRI International maintains a listing of computer abuses. There were only two cases of reported wiretappping in over 700 incidents.[1]

The cost of encryption is also an important barrier to growth. The major elements of cost associated with cryptography are:

- purchase price of the hardware;
- system delays imposed by the use of cryptography; (software for cryption typically involves unacceptable transformation delays);
- training for users, system maintainers, system designers, and others involved with the system;
- key distribution and management;
- backup hardware, procedures and testing;
- documentation of cryptographic system; and
- consulting assistance for system integration (e.g., network protocol and file translation redesign).

---

[1]Charles Cressonwood. "Future Applications of Cryptography". Journal of Telecommunication Networks. Summer 1982, p. 66.

An encrypted communications link requires a DES device at both link ends. One encryption device is at the host computer and a similar device is at each terminal used to access the host computer. Add-on DES devices can cost between $2,000 and $3,500 per terminal with an average price of $2,200 without such options as special key management features. Hardware DES encryption in the form of encryption board technology for personal computers can cost between $400 and $1,500. In addition to the cost of the DES equipment, the management of the keys can be an added and difficult burden. The future of cryptography lies in building the DES into the equipment at the start. The cost would then be less than $100 per terminal for DES security.

Given the costs associated with encryption, it is likely that lower level inexpensive security control will first be implemented previous to encryption. These other controls include:[1]

- multiplexing of transmission lines;
- the use of synchronous, continuous data streams;
- the use of the highest possible transmission speed;
- the use of alternative paths and rotary line configurations, as in a multinodal network;
- block transmission (file transfer) as opposed to single message transmission, similarly, the use of concentrators and multiplexers gives better protection than the standard form of transmission;
- the use of advanced line protocol (BSC, HDLC, SDLC, etc.), requiring many checks to be performed before contact is established between sender and receiver;
- routing protection (especially if the system is active) by encryption of the routing-code tables or the allowance of "off-line" change only;
- terminal identification by the network;
- the usage of "closed-user groups" if possible; and
- linking between network and authentication protocols.

The market outlook for encryption is such that as systems become more secure through more elementary precautions such as those mentioned above, encryption will become increasingly needed to counter the more sophisticated attacks.

---

[1]Bank Administration Institute. Security and Reliability in Electron Systems for Payments. Rolling Meadows, Illinois, 1982, p. 21.

Regulatory and Legislative Pressures

Encryption may soon be warranted in many systems not so much because it is indicated by its economics, but because it will be mandated by a standard of due care. The Foreign Corrupt Practices Act of 1977 legislated that management may be held liable for negligence for failing to install the appropriate communications control measures. The Privacy Act of 1974 and the Office of Management and Budget Directive A-71 have similarly attempted to create a standard of due care for Federal government information and communications systems. In addition, a court case, Peterson vs. Idaho First National Bank, held that "inviolate secrecy is one of the inherent and fundamental precepts of the relationship between the bank and its customers or depositors."[1]

The American Bankers Association (ABA) and ANSI have proposed voluntary standards for the use of DES to protect sensitive financial data. When encryption becomes an accepted prudent safeguard to use in banking systems, a bank could be fined and the board of directors could be held personally liable for the loss of assets that could have been prevented with encryption. The Foreign Corrupt Practices Act holds that officers are personally liable for fines of up to $10,000 and imprisonment of up to five years. The Act also provides for separate civil lawsuits against the bank and its officers.

Encryption may also be mandated in the banking community by legislation. A draft is before the Secretary of the Treasuary, Mr. Donald T. Regan, that would require encryption to be used in certain situations.

Industry Perceptions

Conversations with banking industry officials revealed the key role played by the Bureau in the development of encryption standards. The Chairman of the ANSI Committee X9E8, Mr. Blake Greenlee of Citibank, claimed that the Bureau's work with the financial community in developing security and encryption standards had been responsible for the promulgation of a higher quality standard as well as ensured compatibility between the standards in use in the private sector and those public sector standards used by the Federal Reserve Board and the U.S. Treasury Department.

---

[1]See: "Data Security". The Bankers Magazine. March 1984, p. 58.

An encrypted communications link requires a DES device at both link ends. One encryption device is at the host computer and a similar device is at each terminal used to access the host computer. Add-on DES devices can cost between $2,000 and $3,500 per terminal with an average price of $2,200 without such options as special key management features. Hardware DES encryption in the form of encryption board technology for personal computers can cost between $400 and $1,500. In addition to the cost of the DES equipment, the management of the keys can be an added and difficult burden. The future of cryptography lies in building the DES into the equipment at the start. The cost would then be less than $100 per terminal for DES security.

Given the costs associated with encryption, it is likely that lower level inexpensive security control will first be implemented previous to encryption. These other controls include:[1]

- multiplexing of transmission lines;
- the use of synchronous, continuous data streams;
- the use of the highest possible transmission speed;
- the use of alternative paths and rotary line configurations, as in a multinodal network;
- block transmission (file transfer) as opposed to single message transmission, similarly, the use of concentrators and multiplexers gives better protection than the standard form of transmission;
- the use of advanced line protocol (BSC, HDLC, SDLC, etc.), requiring many checks to be performed before contact is established between sender and receiver;
- routing protection (especially if the system is active) by encryption of the routing-code tables or the allowance of "off-line" change only;
- terminal identification by the network;
- the usage of "closed-user groups" if possible; and
- linking between network and authentication protocols.

The market outlook for encryption is such that as systems become more secure through more elementary precautions such as those mentioned above, encryption will become increasingly needed to counter the more sophisticated attacks.

---

[1]Bank Administration Institute. Security and Reliability in Electron Systems for Payments. Rolling Meadows, Illinois, 1982, p. 21.

Regulatory and Legislative Pressures

Encryption may soon be warranted in many systems not so much because it is indicated by its economics, but because it will be mandated by a standard of due care. The Foreign Corrupt Practices Act of 1977 legislated that management may be held liable for negligence for failing to install the appropriate communications control measures. The Privacy Act of 1974 and the Office of Management and Budget Directive A-71 have similarly attempted to create a standard of due care for Federal government information and communications systems. In addition, a court case, Peterson vs. Idaho First National Bank, held that "inviolate secrecy is one of the inherent and fundamental precepts of the relationship between the bank and its customers or depositors."[1]

The American Bankers Association (ABA) and ANSI have proposed voluntary standards for the use of DES to protect sensitive financial data. When encryption becomes an accepted prudent safeguard to use in banking systems, a bank could be fined and the board of directors could be held personally liable for the loss of assets that could have been prevented with encryption. The Foreign Corrupt Practices Act holds that officers are personally liable for fines of up to $10,000 and imprisonment of up to five years. The Act also provides for separate civil lawsuits against the bank and its officers.

Encryption may also be mandated in the banking community by legislation. A draft is before the Secretary of the Treasuary, Mr. Donald T. Regan, that would require encryption to be used in certain situations.

Industry Perceptions

Conversations with banking industry officials revealed the key role played by the Bureau in the development of encryption standards. The Chairman of the ANSI Committee X9E8, Mr. Blake Greenlee of Citibank, claimed that the Bureau's work with the financial community in developing security and encryption standards had been responsible for the promulgation of a higher quality standard as well as ensured compatibility between the standards in use in the private sector and those public sector standards used by the Federal Reserve Board and the U.S. Treasury Department.

---

[1]See: "Data Security". The Bankers Magazine. March 1984, p. 58.

Mr. Greenlee also conveyed the industry perceptions of the need for an even greater effort on the part of NBS. These perceptions included the need for NBS to:

- speed the development of security standards as there are currently only a handful of people working on all the standards development;
- serve as a testing facility where equipment manufacturers could bring their security equipment to ensure that their equipment complies with the standards. NBS would not endorse their equipment, only provide the testing facilities;
- help develop processing and information standards that would be as important in the service industries as the initial NBS efforts in length, time, and weight were to the manufacturing industries;

In spite of the barriers mentioned earlier, the future outlook for encryption uses is good. As banking operations become more automated, DES will be built into equipment as systems begin to emphasize end-to-end rather than link-to-link encryption for better security.

6

SMART CARD

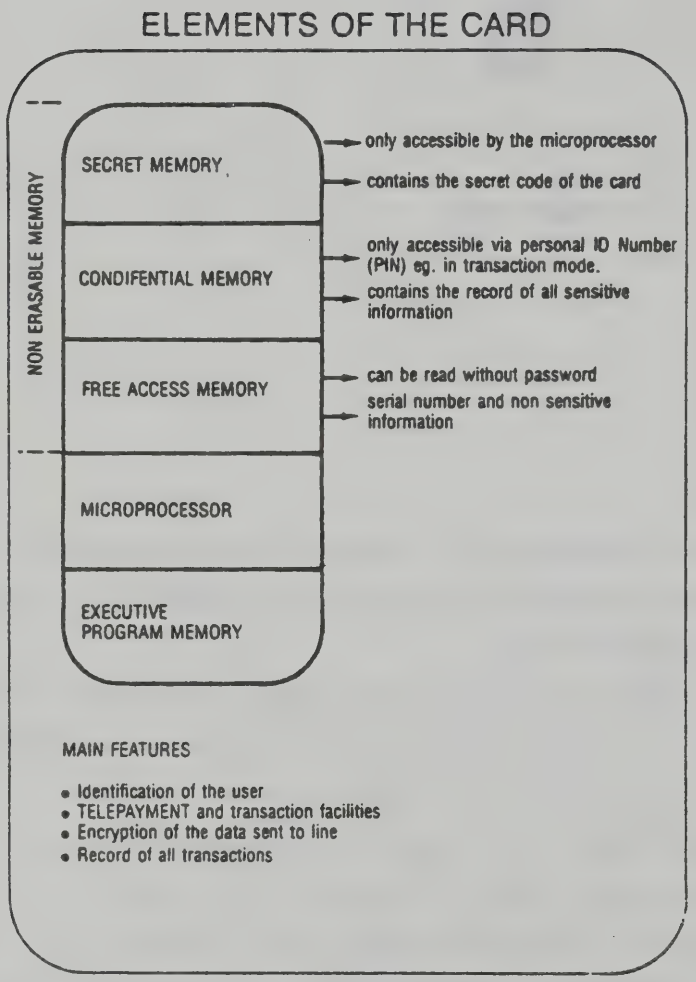
BACKGROUND

The smart card or (carte a memoire) was invented in the mid-1970's by a Frenchman, Roland Moreno. Its use has been pioneered in France by a combined effort of the government and private firms.

As a concept, the smart card has unique advantages as an identification pass, holder of personal data, encryption device, electronic authorization and an electronic payment method. Questions still remain about the smart card and work is continuing on its improvement, but cards now being tested appear to be working well. There is little doubt that by the end of the decade, at least in France, millions of people will use smart cards as a convenient and secure medium for interaction with computers, communication devices, terminals and informational systems.

Description

A smart card basically is a credit card implanted with an integrated circuit chip or chips with nonvolatile memory and computational capabilities. Its elements and dimensions are depicted in Figure 6-1. Permanent microprogramming and manufactured-supplied data is in a read-only memory or in a section of programmable read-only memory that cannot be written on. The memory


ELEMENTS OF THE CARD
NON ERASABLE MEMORY
SECRET MEMORY
only accessible by the microprocessor
contains the secret code of the card
CONDIFENTIAL MEMORY
only accessible via personal ID Number (PIN) eg. in transaction mode.
contains the record of all sensitive information
FREE ACCESS MEMORY
can be read without password
serial number and non sensitive information
MICROPROCESSOR
EXECUTIVE PROGRAM MEMORY
MAIN FEATURES
• Identification of the user
• TELEPAYMENT and transaction facilities
• Encryption of the data sent to line
• Record of all transactions

Technical data

Dimensions :
Conforming with ISO 2894, including thickness : .76 mm.

Personalization :
Printed or embossed.
Optional : photograph
signature.

Magnetic tracks :
ISO 2, ISO 3.

Components :
8 bit microprocessor
2 K 6 bits memory.

Contacts :
8, golden, 6 of which actually used.

Capacity :
Over 150 transactions.

PIN Code :
Randomly attributed at card production.
Changeable once with use of original PIN.
Management of errors by card.

Revolving expenditure limit :
Monthly base
Automatically restored every new month
Changeable by banker once in card life.

Remaining buying power :
Calculated by card for each transaction.

FIGURE 6-1: ELEMENTS AND DIMENSIONS OF SMART CARDS

Source: Intelmatique News Release. Philips Data Systems. 1983.

is segmented into three sections. The first section is inaccessible from outside the card. The second section is accessible for writing or reading under conditions determined by the microprogramming of the card. The third section is open for access to anyone. Present commercially available cards hold up to 12 kilobytes of information. Cards must be replaced after their memories are completely filled. The computational capabilities of the microprocessor are used to execute algorithms, such as personal identification number (PIN) comparisons, message authentication and data encryption operations, and to control the use of the memory.

Point-of-Sale (POS) Application

The smart card was originially conceived as being used in a debit POS system. The French believe that the smart card will replace current payment methods because it offers security against theft and fraud, avoids high transaction costs and provides greater flexibility in use.

In a POS system, the issuing bank will personalize the card with the customer's account number, PIN and secret bank code word. The bank will also establish a monthly spending limit that can be programmed into each card and automatically reset each month.

At the POS, a retailer could establish the identity of the cardholder by the PIN, and determine the availability of funds. If the credit is sufficient and the PIN is okay, then the transaction's amount and date is written into the customer's card. At the same time, the date, amount and purchase account number are entered into a memory cartridge (usually magnetic tape or disk) inside the store's POS terminal. The retailer's entire transaction file can then be delivered either physically or transmitted over telephone lines to the retailer's bank. The memory cartridge can then be erased and updated blacklist information about invalid cards can be reloaded.

Security Aspects

The most important application of the smart card may be for security. Smart cards can have security features that only a computing device could have. Magnetic-stripe and digital optical cards can be made components of security systems, but they cannot have the full security of a device that can execute

programming instructions internally. The Department of Defense has issued the smart card their highest security rating. While smart cards do not offer any more security than other computer systems, they can be upgraded to keep the security features a step ahead of criminal efforts. Because the security is software-based, upgrading will probably not cause the terminals or card interfaces to be made obsolete.

The security functions that can be performed by smart cards are:[1]

- identification of the bearer (typically a PIN comparison);
- encryption or deciphering of messages;
- protection against forged or simulated cards;
- protection of authorizations carried in the card;
- authentication of transactions involving the card; and
- protection of records stored in the card.

The cardholder is identified by entering a PIN through a keyboard where the PIN is compared with the stored cardholder PIN. PIN comparison is entirely within the card itself which is a security advantage over other cards that require the transactional terminal to be secure. If the cardholder fails to enter the correct PIN after a prespecified number of attempts, the card's electronics are blocked and the card is rendered unusable.

A smart card could also store digital physiological data of the bearer for identification purposes such as the bearer's fingerprints, signature, voiceprint or capillary pattern in the eye. These physiological identifiers are advantageous because the information cannot be transferred to another person. While none are currently used, their use is foreseen when they become more reliable, less expensive and more widely acceptable. VISA is seriously considering using signature verification for its electronic POS card in the future.

A smart card can act as a portable encryption device. The secret area of the card's memory can store a cryptographic key, and the card itself can be programmed to encrypt and decrypt transmitted data. IBM sees the card as a likely solution for key handling in cryptography, and in Britain, the National

---

[1] Stephen B. Weinstein. "Smart Credit Cards: The Answer to Cashless Shopping". IEEE Spectrum. February 1984, p. 46.

Physical Laboratory is also looking at the smart card for cryptographic techniques. Work is still needed to allow the Data Encryption Standard (DES) to be carried out. High-speed processors will be needed to execute the more complex algorithm at speeds useful in telecommunications.

The smart card will be more difficult to forge than other cards because of the technical difficulty of manufacturing the chip and the high costs that would be involved in illicit reproduction.

Smart cards can be used from home terminals such as in videotex applications to authenticate transactions and access data bases. In the French videotex system, the holder's bank account number is transmitted to the terminal and to the bank's computer. The bank's computer produces a random number and transmits it back to the card. The smart card's secret code word and the user's account number are used in conjunction with the random number to compute an authentication code in the card. The bank's computer produces a code in parallel and if they are identical, then the user is cleared.

Each card carries an individual serial number, manufacturer's code, secret code words, etc. that are stored in the secret memory compartment at the time of manufacture or when it is initialized under user control. After that, it cannot be changed or read from outside the card. There is a potential for access to the secret memory through unusual power-up procedures and careful monitoring of current drains and electromagnetic fields or by reading with the help of an electronic microscope, but the threats can be minimized by careful design.

Stored records in cards are protected against erasure and overwriting. Such measures also prevent a cardholder from making unauthorized changes. The Honeywell Bull smart card is protected against erasure by ultraviolet light or other radiation by a mechanism that disables the card if it has become irradiated.

One unresolved security problem is for an off-line POS system. The memory provided in the transaction terminal could not accommodate the amount of bad serial numbers that would be necessary for a worldwide card system with tens of millions of outstanding cards. The risk of PIN compromise and bad-credit losses may be serious enough to limit off-line transactional systems using smart cards to small user groups. Physiological indicators such as signature analysis, however, could be one means to diminish the off-line security problem.

PILOT TESTS AND ACTIVITIES WORLDWIDE

This section presents a review of pilot tests and activities of smart cards in the U.S. and overseas. The European experience is reviewed first, followed by a discussion of the American experience.

France

There is major smart card activity in France where a combination of private and public efforts have developed and promoted its application. The smart card was adopted by the French government's Telematique program. Telematique is France's national program to bring the advantages of computer technology and telecommunications to everyone's home or business. Telematique's policy is to coordinate companies and products into a fully-compatible effort so as to fulfill the needs of the informational society and permit greater efficiency. The major French companies that have been developing the smart card are Phillips Data Systems, Cii Bull and Flonic Schlumberger.

Smart cards are currently used in France for:

- POS transactions;
- telepayment in videotex services;
- public telephone payment;
- decoders for French pay TV; and
- medical and educational record-keeping.

The French Postes, Telephones, et Telegraphs Ministry (PTT) has announced that it will implement 1.5 million multiservice smart cards during 1984 that can be used in banking, videotex, telephone and television decoding operations.

A debit POS system has guided the French smart card effort. A consortium of major French banks and the PTT has plans for the smart card to automate checking and reduce check processing costs as it replaces the checkbook. Three separate POS trials were started in 1982 and is still continuing in the cities of Lyon, Caen and Blois with a total of 120,000 cards and 650 retail terminals being used. Currently, the smart cards used in the three separate POS trials are incompatible, but in the future, the cards will have the same interchange protocols.

The two largest credit card organizations in France, Carte Bleue (associated with VISA International) and Carte Verte (associated with Eurocard/Mastercard) have agreed on the distribution and promotion of a single payment card combining the smart card and magnetic stripe technology. Approximately one million "smart stripe cards" will be issued by 1985 to be used for POS and ATM terminals. The Carte Bleue organization expressed that they were persuaded to use the smart stripe card as it satisfied the following criteria:[1]

- Growing mass market use of their services demanded a universal solution, i.e., smart stripe card;
- Provided for improved security and privacy;
- Non-erasable memory will stop false claims by customer;
- The POS trials have provided evidence of high reliablility; and
- Will speed up and simplify the transaction process.

In an agreement with the French PTT, the 3.3 million Carte Bleue customers will be able to use their card in the 450 Giro Bank cash dispensers, and the 7.6 million Giro Bank customers would be able to use their smart cards in the 190,000 retailers affiliated with Carte Bleve.

The present tests of videotex and smart cards are using the Minitel terminal, a low-cost, stand-alone terminal that is used in France's electronic telephone directory and Teletel videotex services. In addition to home banking services, Teletel customers can order and pay for goods from mail-order houses and make railway seat reservations with their smart cards. The telepayment cards have an encryption mechanism to guard against fraud and to protect the privacy of banking transactions. The French PTT intends to order 50,000 smart card readers that can be attached to videotex terminals, 50,00 terminals with integrated card readers and 200,000 videotex telepayment smart cards.

Smart card telephone booths will begin to be installed in France in 1984. Approximately 2,000 are due to be introduced this year and 100,000 are planned to be in place by the end of the decade. Orders have been placed for 250,000 telephone cards. Two types of smart cards will be used. Prepaid cards will be anonymous and be programmed for a set amount of dollars that will be debited

---

[1]Roy Bright. "Smart Card Beats an Ace in the Hole". Intelmatique News Release. February 1984.

until the card is exhausted. The second type are personalized credit cards. Telephone charges will be recorded in these cards and automatically transferred to a billing center at prescribed limits. By batching these calls in the smart card's memory, the disproportionate cost of processing small value transactions will be overcome.

Smart cards are being used at Paris University for 5,000 students to record courses taken and credits earned and to enroll in classes. The university plans to extend the smart card to all of its students and may use it to record the payment of school fees and as a specialized access pass.

Smart cards will be used to maintain individual vaccination records for all students in Blois, and card readers will be issued to the city's schools and physicians. It is planned that an individual health card will eventually be created for every French person.

Germany and Sweden

West Germany's PTT, the Bundespost, is currently studying applications of the smart card in its videotex service known as Bildschirmtext, and for the public phone system. Primarily, the Bundespost hopes to determine whether the smart card can solve the problem of maintaining security while giving access to diverse services and data bases in their videotex system.

The Bergen Bank of Norway and the Norwegian telecommunications authority are collaborating for a smart card test in 1984. The test will be of multiservice use including public pay phone, POS and videotex telepayment applications.

United States

There has been very little activity regarding the smart card in the U.S. In the Spring of 1983, Smart Card International of New York City was the fourth company to be granted the patent rights to the smart card. The firm is the only American firm and first non-french firm to have the authorization to produce or sublicense others to produce smart cards and terminals.

Other U.S. firms have shown an interest and could be potential manufacturers of smart cards. The IBM Corporation has held a patent on an information card since 1972 and may be a potential manufacturer of smart card systems. DataKey, Inc. of Burnsville, Minnesota -- maker of keys and military dog tags -- have

expressed an interest in smart cards. Smart Card Systems, Inc. of Cherry Hill, New Jersey is aiming to produce a 64K byte card (not necessarily rewritable) by 1986. Corpra Research of Philadelphia, specializing in smart card applications, has also expressed an interest in manufacturing smart cards.[1]

Financial institutions which have investigated the use of smart cards include First Bank System Inc. of Minneapolis (which used very few smart cards in their videotex pilot), Chemical Bank, Citicorp, Bank of America, the New York Stock Exchange, Security Pacific Bank, American Express (conducting an in-house test of smart cards), and Chase Manhattan Bank (tested card in Europe).

The Federal government is interested in the smart card but so far has not conducted any conclusive tests. Smart cards were tried in the Realtime Automated Personnel Identification Card System (RAPIDS) program which was mandated by Congress to eliminate fraud, waste and abuse of ID cards used in the military. The test was inconclusive as the smart cards were used as ordinary plastic cards and were not tested for their unique abilities. The Department of Agriculture announced that they were going to test the smart card in their POS food stamp pilot but then withdrew the smart card from the test. The Federal government has mandated that smart cards be tried again in a test that will demonstrate the card's potential.

BARRIERS TO ADOPTION AND USE

Adoption of the smart card will not come as easily to the United States as in France. The government and banking cooperation that helps to ensure uniformity and acceptance of the technology in France will be difficult to replicate in the U.S. The two major barriers to the smart card are the cost of the card itself and the infrastructure necessary for it.

The cost of the smart card is becoming less of a barrier. In 1982, cards were priced at $11 in batches over 10,000. They now are priced at $2 to $10, and depending upon the card's capabilities and quantities manufactured, prices should continue to decline in the future.

Meanwhile, the cost of standard magnetic cards (presently, about $.75) are rising due to the extra security measures being added to the card, including

---

[1]Stephen B. Weinstein. "Smart Credit Cards: The Answer to Cashless Shopping". IEEE Spectrum. p. 44, February 1984.

hologram insignias, microprinting and graphics visible only under ultraviolet light. These security devices are needed as credit card fraud is dramatically rising. The smart card's increasingly low price and the potential savings in fraud loss through its enhanced security features will make it more economically attractive in the future.

The infrastructure already in place in the financial community is based on magnetic stripe technology and will not disappear in the foreseeable future because of the enormous investments associated with it. Thus, any new technology must be compatible with magnetic stripe technology and slowly replace it over time. The smart card meets this criterion as it is compatible with magnetic stripe technology. France's two leading credit card companies will introduce just such a smart card combined with magnetic stripes. The so called "smart stripe card" will allow the smart card to be introduced without abandoning the huge investment in magnetic stripe technology.

Most experts monitoring smart card developments think that banking will not be the first U.S. user of the technology but that adoption will first come in closed-end situations where the card will fulfill needs not presently met. One such area is the medical field where a smart card could authenticate claims and carry personal medical histories.

Arlen Lessin, President of Smart Card International, says that his company is developing applications customized to the specific requirements of various user groups and feels that the Federal government offers one such opportunity as most of the government is still operating on paper-based technology.[1] Roy Bright, Managing Director of Intematique, the French organization that has worldwide responsibility for marketing and promotion of the smart card, does not expect the banking community to be in the smart card's first wave of acceptance. But he believes that financial organizations that are experimenting with the card will gain invaluable experience, particularly regarding security, for the future.[2]

There are specialized areas where banks could immediately use the smart card. These include high dollar money transfers and home banking situations.

---

[1]Jean Young. "What's Happening With Smart Cards"? Bank Administration Magazine. January, 1984. p. 30.

[2]Ibid. p. 30.

STANDARDS ACTIVITIES AND TECHNICAL SUPPORT NEEDS

To expedite progress in standards, a multinational organization International Association for Microcircuit Cards (INTAMIC) was established in France in June 1981. Its members include banks and other financial institutions from several European countries, the Far East and the United States, including Chase Manhattan Bank and Bank of America. INTAMIC has taken over most of the conceptual and technical development functions of the smart card. The International Standards Organization (ISO) is where most of the standards efforts are concerted with active members from the U.S., United Kingdom, France, Japan, Germany, and other Western European countries. Using INTAMIC and other government's inputs, the ISO has developed a draft standard for the physical interface, and a draft proposal on data interchange between cards and readers. The smart card meets ISO specifications, having the same size, flexing capabilities, survival over a wide range of temperatures and humidity, and thickness, of ordinary plastic credit cards. Smart cards are also compatible with embossing and magnetic stripes to ensure duality of use for presently magnetic stripe-based operations.

AFNOR is the official standards-setting body in France and has an active smart card working group. AFNOR is the secretariat and chair for ISO working group 97/17/4 on the integrated-circuit card.

In the United States, the American National Standards Institute (ANSI) X3B10.1 committee will handle the physical and technical issues of the smart card and act as a liaison to ISO. Tom Thomas of the U.S. League of Savings Institutions and Chairman of the ANSI X9A committee on retail banking, expressed that once smart card standards are determined, there will be a need for a test facility run by a non-biased third party to determine if manufacturer's cards meet the specified standards. He said NBS could provide such a service, which would be comparable to the magnetic tape comparison that NBS provides for credit cards.[1]

FUTURE OUTLOOK

Work is needed for the smart card to carry out complex algorithms, such as those specified by the DES. Cards will have greater memories. Experimental

---

[1]Tom Thomas, from a telephone conversation on March 29, 1984.

Japanese cards have been demonstrated with a 16K byte capacity. Cost and possibly heat dissipation are the major barriers to making large memory cards. An electrically erasable smart card would benefit many applications as new data could keep coming and old data periodically erased. Better and cheaper card readers are needed. Some would like to see a hand-held card reader and calculator, which would make the contents of the card accessible to the owner.

7

HOME BANKING

BACKGROUND

Home banking systems have generally received the most favorable reviews of all videotex services among consumers. Home banking is attractive to customers as it can provide both cost and convenience benefits for their existing banking needs and can offer services which were unavailable before. The following is a list of services which could be made available:

- balance inquiries,
- credit card account status,
- loan requests and status,
- automatic payment of recurring expenses such as a mortgage,
- bill payment to participating merchants and utilities,
- on-line investment planning,
- account maintenance - place a stop payment, place a check order, and
- funds transfer - both interbank and intrabank.

The more integrated and on-line mode operations a bank is, the easier and less costlier it will be to participate fully in home banking. The major factor that will preclude a rapid development of a broad spectrum of financial services will be the possibility of a security breach. Large funds transfers, investment orders and portfolio histories will probably not be included due to security fears.

Home banking is also attractive to financial institutions for several reasons:

- It offers banks the opportunity to introduce a broad range of financial related fee based services which can increase their revenues.
- It can reduce banks' paper and labor costs associated with monthly statements, teller transactions and check processing.
- It offers banks an inexpensive alternative to the building and staffing of new bank branches.
- Home banking allows financial institutions to compete in new markets and keep abreast of the competition.

Consequently, most of the nation's leading banks, including Bank of America, Chase Manhattan Bank, Chemical Bank, Banc One Corporation, Citibank and a number of larger regional banks, are all pursuing the home banking market.

The precedent of banks being involved in videotex services can be seen when looking at other nations videotex systems. A study by Link Resources[1] of 45 of the world's public videotex systems found that banks were the largest category of information providers to videotex services. Banks were also among the first to make use of response facilities by setting up home banking services.

Banks will not be the only organizations that will bring financial services to homes. Brokers such as Merrill Lynch, computer service companies such as Automatic Data Processing (ADP), and retailers, including Sears Roebuck, and Company, are also planning to provide financial services to homes. Therefore, although home banking offers tremendous opportunities to banks, they will have to compete aggressively for the new market with brokers, retailers, and system operators.

Organizational Options for Bank Involvement

Once a bank decides to get involved in home banking, it has several organizational options from which to choose.

A bank may choose to be only a provider of information and transaction services, and pay to use a videotex system. This method requires the least commitment of a bank. Another alternative is a syndicated approach where a bank

---

[1]"New Link Resource Study on Worldwide Videotex/Teletext". Videodisc Videotex. Summer 1983, p. 175.

shares the cost with other organizations. An example is the ADP Home Banking Interchange where 20 or so banks have joined ADP's program to test home banking in their areas.

A bank or banks may also create a financial gateway to a videotex system and earn fee income from other banks. Such an example is the four banks who joined together to create the Video Financial Services gateway to the Viewtron system.

Another alternative would be for a bank to independently implement a home banking service. An example is Chemical Bank's Pronto system. Chemical Bank is also in a vendor situation as it franchises out the hardware and software of the Pronto system to other banks.

It can be advantageous for banks to be a system operator because of the potential fee income that can be derived by being the payment processor for all videotex services. Regardless of how useful consumers perceive home banking to be, there is a limit on the amount of fee income that can be generated. However, by operating the system themselves, banks would be in the position to be the payment processor to other videotex services, such as, informational retrieval, home shopping and electronic mail, and earn income on virtually every videotex transaction.

An example of the above is a customer in Los Angeles who uses the Dow Jones News Retrieval Service at a cost of $2.50. Dow Jones must generate a bill and send it to the customer. The customer writes a check and sends it to Dow Jones in New Jersey, where it is processed and deposited by Dow Jones, then sent through the Federal Reserve Systems Clearing House, and finally presented to the customer's Los Angeles bank for payment. If, however, the customer's bank served as the payments processor for his videotex system, at the conclusion of the search the bank would ask the customer whether to charge that amount to his savings, checking or credit card account. The bank would then transfer the payment electronically to Dow Jones. In addition to providing benefits to all parties, the bank can charge a service fee to Dow Jones for collecting and transferring the funds to Dow Jones' bank.

PILOT TESTS AND INDUSTRY PARTICIPANTS

As many as 12 pilot tests of home banking operations have been conducted during the last four years. Some of these pilot tests, shown in Table 7-1 have

Table 7-1: Home Banking Trials in the United States

	Financial Institution	Location	Project Name	Participants	Status
Automated Data Processing (ADP)	25-50 banks nationwide	various U.S. locations	Home Banking Interchange	5,000	on-going
Banc One	Banc One	Columbus, OH	OCLC Channel 2000	200	ended 1981
Chase Manhattan	Chase Manhattan	New York City New Jersey, & Connecticut	Chase Home Banking	300	pilot
Chemical Bank	Chemical Bank and 8 other nationwide banks	New York City	Pronto	2,000	on-going
Citibank	Citibank	New York City	Home Base	100	pilot
ContelVision	Commonwealth Savings & Loan Association, Piedmont Federal Savings & Loan Assoc.	Manassas, VA	ContelVision	100	ended 1983
Cox Cable	California First Bank, First Interstate Bank, Security Pacific, Home Federal Savings, San Diego Federal Savings	San Diego, CA	INDAX	300	ended 1983
First Bank System	First Bank System	Minneapolis, MN; Fargo, Wahpeton, and Valley City, ND	Firsthand	300	ended 1983

Table 7-1 (continued)

	Financial Institution	Location	Project Name	Participants	Status
First Interstate Bank of California	First Interstate Bank of California	Los Angeles & San Fernando, California	Video Banking	250	ended 1982
Times-Mirror	Bank of America	Southern Calif.	Gateway	N.A.	ended 1983
United American Services Corporation	United American Bank	Knoxville, TN	Bank-At-Home	400	N.A.
Viewdata Corporation	Video Financial Services	Coral Gable, FL	Viewtron	5,000	on-going

N.A. denotes information not available.

Source: Information was obtained from John Tydeman, et. al. Teletext and Videotex in the United States, p. 241 and O. Tom Thomas, "Home Banking's Progress Stalls". Savings Institute. July 1983, p. 126.

progressed to commercial operations. The most important pilot tests and ventures are discussed below.

Home Banking Interchange

Home Banking Interchange (HBI) is a cooperative venture of approximately 25-30 banks and ADP Telephone Computing Services, a subsidiary of the ADP Corporation. HBI has assembled a complete videotex package that banks will use in their pilot studies of home banking. Videotex American -- part of Times-Mirror -- will supply the news, sports, weather, and shopping of the service. HBI was used in the Venture One CBS/AT&T pilot in Ridgewood, New Jersey and for the City Trust home banking pilot in Bridgeport, Connecticut. Additional pilots are scheduled for 17 banks in Arizona and six banks in Ohio.

Video Financial Services

Video Financial Services is the financial gateway to the Viewtron videotex system in Southern Florida. The gateway is owned by four banks: Southeast Bank of North America (Miami, Florida), The Wachovia Corporation (Winston-Salem, North Carolina), Security Pacific Corporation (Los Angeles, California), and Banc One Corporation (Columbus, Ohio). Video Financial Services provides home banking services and sells it to other banks. The gateway works similar to an ATM switch.

Video Financial Services includes bill-paying for every participating organization, supports authorization of all major credit cards, national and proprietary debit cards, and supports transactional banking. It also offers settlement between the banks, both intra- and interbank. It supports commercial banks, savings and loans and credit unions on-line and off-line.

Some 13 Florida banks have signed up to offer banking on the system. The banks pay a one-time membership fee of $10,000 and a fee of $4-$5 per month, per customer. Viewtron gets a flat fee and Video Financial Services gets a user-based fee. Each bank chooses what their organization will offer on the system. In addition to the fees that are charged, a bank's cost will depend upon how they link up with Viewtron. The bank can produce an off-line strip file for their customers or a bank can provide a direct on-line attachment to Viewtron's host computer. The first method is currently used by all of the banks because

it is inexpensive. The second method, while operationally superior, is too expensive for the small number of customers presently on the system. It is estimated that a bank's activities will have to rise to 2,500-3,000 transactions per month before it will be economical to invest in data processing expenses to convert to an on-line mode.

Pronto

Chemical Bank, the nation's sixth largest bank has developed the Pronto Home Banking system at a cost of $20 million by the end of 1983. The system had been tested by 200 users in New York since November 1982 and was launched commercially to the public in September, 1983. Over 2,000 users currently use the service.

Pronto can be used for bill paying, bank balance inquiry, funds transfer, bank account statements, budgeting, electronic mail, and an electronic cash register. Bill paying is probably the most important function Pronto can offer as the average consumer receives 150 bills per year. More than 400 New York area and national merchants accept payment from the home banking system, including major department stores, credit card companies, utilities, and large landlords. An electronic mail service allows messages to be sent by customers either to the bank or to one another. In addition, the bank can contact customers individually or as a group. Pronto is expected to have in the future other services including news, educational services, catalog shopping, weather and stock quotations.

To ensure continuous, reliable security, Chemical Bank runs Pronto on a Non-stop II computer system from Tandem Computers, Inc. Tandem builds fault-tolerant computers that are designed to keep on working even if a processor fails.

To use the Pronto home banking service, a customer needs a home computer with a modem hooked up to a telephone, and a television set or display terminal. Pronto can only be accessed now on an IBM, Apple or Atari personal computer. In the future, the system should be terminal indifferent. The system also works better with an intelligent modem. The service costs customers a $12 a month fee. A user receives a special communications software cartridge or floppy disk that is inserted into the home computer, and instructs it to automatically dial into the Tymnet public packet-switching network. Security is provided by a terminal identification that is embedded in the customer's special software, a household identification, a person's code name, and a personal identification number (PIN).

Chemical Bank has licensed Pronto to eight banks thoughout the United States that will test the Pronto system. On a 200-household test of Pronto, a bank pays a $25,000 licensing fee, plus about $100,000 to cover the cost of installing a dedicated phone line to Chemical's computer, hooking into a packet switching network and adding local computer hardware. After a test, a bank can have a permanent license for a fee of $75,000. There is also a software maintenance fee of $10,000 a year and a fee of $1 a month for each Pronto customer. Pronto will probably not become cost efficient for a bank until it has 15,000 to 20,000 customers.

Bildschirmtext

One of the most highly praised home banking services is offered by the Vaubraucher Bank in Hamburg, Germany. More than 2,200 customers of the bank subscribe to the home banking service by a gateway to the German videotex service Bildschirmtext. Customers can receive up-to-date account information, create Giro payments, request money orders, stop checks, receive a status of available lines of credit, and send messages to the bank regarding any questions they may have about any service. To provide security, a person accessing the system must enter an account number and a PIN. When placing transactions through the system, customers must use a ten digit transaction code next to each payment. The bank automatically sends 100 random codes to a customer at the beginning of the session.

MARKET PROJECTIONS

Projections of the growth of the home banking market are presented in Table 7-2. Home banking projections are closely tied to the growth of the home computer industry, because of the relatively high costs of terminal equipment to the consumer. Home banking revenues are projected to $850 million in 1995, not an inconsequential market.

Another market projection of home banking was provided by a year-long study conducted by the Bank Administration Institute and Arthur Anderson and Company[1]

[1]Katherine L. George. "Savings Institutions Begin to Test Electronic Waters of Home Banking". Magazine of Bank Administration. January 1984, p. 30.

study which surveyed hundreds of banking and financial service leaders. The consensus was that home banking will be offered by fewer than 20 percent of commercial banks by 1986 and probably will not be profitable by 1990. Bank panelists predicted that five percent of households would utilize home banking in 1986, increasing to 11 percent in 1990.

Table 7-2

HOME BANKING MARKET PROJECTION

	1987	1995
Percent Households With Videotex	6.0%	20.0%
Home Banking Revenues (million $)	$85	$850
Percent of Total Videotex Revenues	8.5%	14.0%
Revenue Per Month Per Customer	$1.26	$3.75

Source: Predicast Inc. U.S. Videotex and Teletext Markets. Cleveland, Ohio, 1983, p. 64.

Frost and Sullivan,[1] project electronic home banking hardware, software, and service sales to grow to $5 billion by 1991. The key to the market growth will be the spread of microcomputers. Some 75 percent of all commercial banks will become information service providers by 1991.

The potential videotex income that could be derived for transactional expenditures such as home banking and bill-paying, teleshopping and remote reservations has been estimated by John Tydeman and is presented in Table 7-3. The Direct Mail Marketing Association estimated that over 85 million catalogs are sent to consumers a year and that $36 billion are spent on products sold by direct mail marketing. Non-store retail sales are growing at a ten to 15 percent annual rate, more than twice the rate for retail stores. If only a fraction of this market could be captured by videotex, teleshopping could become a major application area.

[1]"Lifestyle and Leisure". Technology Update. February 18, 1984, p. 18.

[2]John Tydeman, et. al. Teletext and Videotex in the United States. McGraw-Hill Publications Company, 1982, p. 74.

Table 7-3

TRANSACTION EXPENDITURES IN POTENTIAL MARKETS FOR VIDEOTEX

	Total 1980 Expenditures ($ billions)	Average Household Expenditure Per Month	% Estimated Annual Growth 1980-1990
Banking and Bill Paying			
• Banking Fees	1.95	$ 2.05	3.6
• Postage for Payment of Bills	1.20	1.25	2.8
Teleshopping			
• Direct Marketing Sales	36.00*	37.50	10.0
Services Requiring Reservations			
• Airline Travel	6.60*	6.90	3.9
• Vacation Lodging	4.95*	5.15	3.8
• Entertainment	14.65*	15.25	3.7

*These figures represent the total values of goods and services purchased.

Source: John Tydeman, et. al. Teletext and Videotex in the United States. McGraw-Hill Publications Company, 1982, p. 74.

To further provide transactional applications via videotex, a home printer would be desirable. A 1981 study conducted by the University of Southern California using delphi techniques was aimed at the ten most likely events that would affect the consumer finance industry. The study panel consisted of 50 leading planners in the nation who predicted that the most likely event would be a low-cost home printer.[1] The printer would open up a whole new dimension of statement printing, coupon printing, tickets, and other services in the home.

BARRIERS TO GROWTH

A number of problems and barriers to the growth of home banking services are noted. Some of these barriers are economic in nature, others involve legal and regulatory problems.

[1]Dale L. Reistad. "Home Banking: Alternative Strategies". Home Delivery Services. Bank Administration Institute, Rolling Meadows, Illinois, 1982, p. 50.

Costs of Bank Participation

It appears that home banking operations, requiring investments close to $10 million will only be marginally profitable at least in the short run.

A study of the economics of home banking conducted by Communications Studies and Planning (CSP) International concluded that:[1]

- Hardware costs for banking at home will decline at a real rate of five to eight percent per year over the next five years and software costs will remain stable.
- Cost reductions could be 28 percent for highly automated banks. Larger savings of up to 90 percent could be achieved as a result of processing consumer loans.
- Anticipated costs of marketing any video home banking program will be $200-$300 per customer.
- For a bank to create its own video banking system from scratch, including all the hardware, will cost an average of $7-$10 million. If it does its own processing, the bank would need 52,000 video banking customers to break even.
- A bank can buy the video banking software at an average cost of $100,000. If it does its own processing, the bank will break even at 25,000 video banking customers.
- A bank that buys its software and contracts with a third party for processing, needs 13,000 video banking customers to break even.

CSP International concluded that home banking will be only marginally profitable at best for the next five years. CSP feels the increasing use of home computers and other videotex services will have a significant beneficiary impact on home banking. The study stressed that while only marginally profitable, other factors such as potential cost-savings and inter bank competition will be incentives for home banking.

Banks will begin home banking on the convenience aspects for their customers and not on a cost-justified basis. This will be similar to the case of the automated teller machines (ATMs). Banks will use home banking to maintain the segment of the affluent retail customers base that provides the greatest share of retail bank profits. An old saying in the banking profession is that 20

[1]"Are Banks Really Ready for Video Banking". ABA Banking Journal. December, 1983, p. 79.

percent of your customers account for 80 percent of your profits. These customers are also likely to have terminals in their home, and will thus become a natural market for home banking services

Costs to the Consumer

The main barrier to the consumer will be the equipment related costs of videotex. At present, videotex terminals of limited graphic capabilities are being offered at $500-$600 per unit in some commercial videotex services. In some videotex options the consumer will have to purchase decoders ($600), modems ($200), and printers ($200-$300). Because of these significant costs to the consumer, the growth of home banking services via videotex will be dependent on the growth of home computers. Those consumers with home computers will become the obvious clients of home banking services.

Regulatory Problems

In 1980, Congress passed the Depository Institution Deregulation and Monetary Control Act. The implications of this act include:

- Higher rates paid on checking and savings deposits of consumers. All interest rate ceilings will be abolished by 1986.
- Reflection of the true cost of banking as consumers will pay actual cost of check processing.
- Less differentiation between commercial banks and thrift institutions.
- Less geographic controls on banking.
- More competition among depository institutions and non-banking institutions such as American Express, Sears Roebuck and Merrill Lynch.

Videotex and home banking impacts all of these issues. Videotex renders geographic controls such as interstate banking restrictions moot, as it makes the geographic proximity of the participants (bank, customer, merchant) irrelevant. Some of the legal problems arise because the laws were enacted without videotex in mind. The recent Electronic Funds Transfer (EFT) Act was drafted with ATMs point of sale (POS) terminals, and telephone bill payment in mind, but not home based terminals. The EFT Act requires that a receipt be made

available to the consumer at the time of transaction. Congress specifically exempted telephones from this requirement, but not-home based terminals. Home banking service providers had to lobby the Federal Reserve for an exemption. A similar exemption from state laws and regulations may be necessary in those states that have receipt requirements in consumer protection laws.

The conflict between banks and non-banks will increase as videotex facilitates the entry into the financial services business by institutions with no experience in traditional banking. In the March, 1982 issue of Deregulation, the chief executive of Sears, Roebuck and Company, Edward Telling, stated that "Financial institutions and other businesses now face a Darwinian process of survival of the fittest in a marketplace that calls out for new products, new services, new ways of doing business." Sears position in both the retail and financial services could prove a very formidable threat for traditional bankers. The recent joint venture between Sears, CBS, and IBM to provide videotex services is icing on the cake for the argument that videotex will provide further competition to banks by outside industry participants. Because of the in-roads into conventional banking by other financial service companies, Congress may enact legislation to allow banks to compete in previously prohibited areas such as offering securities, insurance underwriting, and real estate activities.

The cost of banking to consumers will rise as they realize the true cost of the check payment system. The costs to banks will also rise as they have to pay higher interest rates on checkable deposits and the costs of check processing increase. Consequentially, both consumers and the banks will turn to electronic funds transfers to minimize costs. Home banking will provide for the ultimate retail electronic funds transfer to help reduce the payment costs.

The deregulation of the banking industry will bring about broad changes that can be found in any deregulated industry. These are:[1]

- An increase in performance variability among firms within the industry.
- Increased price pressure on the previously most profitable products.
- Unbundling of products, with a proliferation of new, complex products/service trade-offs.
- An industry-wide profit squeeze forceing rapid cost cutting, particularly in the form of staff reduction.

---

[1]Robert E. Ryan and Henry Hobson. "Justifying Telephone Bill Payment". Home Delivery Services. Bank Administration Institute, Rolling Meadows, Ill, 1982, p. 33.

Low-cost producers will enter the industry towards price sensitive segments of the market. In the airline industry, companies such as New York Air and Peoples Express entered target segments of the market and competed with the main carriers, often pricing at only half the cost of the pre-deregulated price. In banking, a significant number of new low-cost firms, such as Money Market Funds, may take commodity transactions, especially deposits and money market loans, out of the traditional banking system. This would leave banks increasingly originated toward longer term lending and fees for service.

Thus, deregulation will have the banking industry caught between two competitive pressures. The first one will be to hold on to their existing markets by competing against Money Market Funds, etc. The second will be to compete for the new market of videotex services against brokers, retailers, and system operators. As their existing markets shrink, banks will be forced to compete more aggressively in new markets such as videotex or risk losing control of the payment mechanism system.

Liability Problems

A policy issue that will have to be decided is who will have the responsibility for a transaction. If a transaction is lost or unauthorized, will the service provider, system operator, network provider, credit provider or end user be liable for it. Under the existing EFT Act, a bank will bear most of the losses from an unauthorized transaction unless it can prove the transaction was authorized. To protect against such losses, audit trails will be particularly important in video banking systems since the procedures are new and paperless.

Another problem for banks is reversing a video banking payment. It will be difficult for banks to back out of a payment due to insufficient funds once the payment has gone to the merchant. This problem can arise if a system does not operate in real time but uses the memo post arrangement that is common with most ATM and teller-terminal systems.

Privacy and Security Problems

There will be three areas that will come under security and privacy precautions: the customer's terminal, the transmission network, and the system operator. Considerations that will need to be addressed are:

- unauthorized access of the system,
- unauthorized use of personal data and transaction patterns for commercial purposes (e.g., mailing lists and market research),
- retention period of data, and
- conditions under which government entities (e.g., Internal Revenue Service and Social Security) may have access to data and transactions.

Privacy and security would be made easier if only banks operated the system, offered only banking transactions, and used equipment dedicated exclusively to banking purposes. Thus, the operation would be covered by present fiduciary and legal duties. As videotex systems usually will involve many financial and non-financial organizations offering a variety of services, problems of security and privacy become more acute.

Currently, personal data are kept in separate organizations -- in banks, insurance companies, credit card accounts, retail stores. If a videotex system would unify these accounts, there will be great pressure to compile consumer financial profiles for marketing and credit decision purposes.

The transmission network will have to be secure from electronic eavesdropping. The most vulnerable point will be between the home terminal and the first central office, i.e., the local loop.

The Viewtron system in Florida was the first videotex system to make use of the Data Encryption Standard (DES) to provide security and privacy when transmitting banking data. The DES was chosen over the RSA public key algorithm "...because of the lowered computational load, the availability of LSI devises for implementing the algorithm, and the widespread understanding, use and acceptance of the method..."[1] A 64-bit cipher feedbank mode of operation is used for the DES algorithm. This mode requires an error-free communication link since both the encryption and decryption must remain in perfect synchronization. Error detection is achieved by the use of HDLC between the terminal and the network, and with X.25 from the network, through the system switch into the host videotex computer system.

A user can select his own private key and transmit the key to the host computer such that the host is never able to see the secure key in the clear. This was made possible by a Secure Data Encryption Module (SDEM) that is attached

---

[1]Dennis Hall, William Ritter and Edward Poletto. "Applying Data Security to the Videotex Industry". Videotex 83. On-Line Conferences Limited, Publication, England, p. 61.

as a peripheral device to the host computer. The module has secure internal keys which allows only the device itself to decrypt the information. The module uses the clear secret key only in algorithms physically internal to the module.

A hierarchy of accounts was devised so that the highest level secret keys are known only to the module itself. In this way, system operators can let officials from participating banks securely create their own secret keys, which will in turn allow these officials to create secure keys for trusted employees to create secret keys for customers.

The customer's secret key itself is never transmitted over the communication link and the key used by the DES algorithm varies from session to session. This is accomplished by having the security module select a 56-bit random number for use as the DES session key. The random number is encrypted by using the consumer's secret key. The encrypted random number is then sent over the communication link to the user's terminal where he enters his secret key. The random number can be decrypted correctly only if the user has entered the proper secret key. The random number is then loaded as the DES key for the session and the cipher feedback encryption mode begins. The random number is encrypted using itself as the key and this encrypted cipher text is transmitted to the host where the security module can compare the results to determine the proper random number has been returned.

In present home banking and videotex systems, the method of user authentication is a numeric or alphanumeric code. Possession of a card is not necessary to initiate a transaction. As the use of videotex systems for financial transactions becomes more widespread (e.g., electronic checkbooks, electronic funds transfer, and electronic credit cards), system security will become more of a concern and will likely promote the use of a more secure system than just a password. One possibility would be to use a smart card. The home smart card reader could serve an identification purpose and also be used for the payment of goods. In addition, smart cards could greatly simplify the log-on procedures to data bases.

NBS-114A (REV. 2-8C)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET (See instructions)	1. PUBLICATION OR REPORT NO. NBS GCR 84-474-3	2. Performing Organ. Report No.	3. Publication Date October 1984

4. TITLE AND SUBTITLE

Technologies in the Service Sector
Volume III: A Case Study of Payment Technologies in Banking

5. AUTHOR(S)

Armando M. Lago and Elliott E. Hamilton

6. PERFORMING ORGANIZATION (If joint or other than NBS, see instructions)

Ecosometrics, Incorporated
4715 Cordell Avenue
Bethesda, MD 20814

7. Contract/Grant No.
NB83SBCA2084

8. Type of Report & Period Covered
Final

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (Street, City, State, ZIP)

National Bureau of Standards
Department of Commerce
Gaithersburg, MD 20899

10. SUPPLEMENTARY NOTES

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT (A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)

In Volume I, the economic structure and trends in the U.S. service sector are reviewed as a basis for identifying and characterizing technology flows into this sector. The sources, transfer channels and utilization patterns are described as a basis for developing forecasts of the impacts of technology on the various components of the service sector.

Characterization and forecasts of technology trends are used to assess technical and economic barriers to technology-driven productivity growth, including measurement- and standards-related barriers. Two case studies, Videotex/Teletext (Volume II) and Payment Technologies in Banking (Volume III), provide more detailed analyses of two of the more dynamic subsectors.

12. KEY WORDS (Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)

Banking; barriers; communications; growth forecasts; payment technologies; productivity; service sector; technology; technology diffusion; videotex/teletext.

13. AVAILABILITY

☒ Unlimited
☐ For Official Distribution. Do Not Release to NTIS
☐ Order From Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.
☒ Order From National Technical Information Service (NTIS), Springfield, VA. 22161

14. NO. OF PRINTED PAGES

15. Price